Audit Report

SUMMARY OF AUDIT RESULTS--DOD INFORMATION ASSURANCE CHALLENGES

Report No. 99-069 January 22, 1999

Office of the Inspector General
Department of Defense

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: **Summary of Audit Results--DoD Information Assurance Challenges**

B. DATE Report Downloaded From the Internet: 09/03/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 09/03/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932 or visit the Inspector General, DoD, home page at: www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Audit Followup and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, Virginia 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

AFMC	Air Force Materiel Command
CIO	Chief Information Officer
C^4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
DCPDS	Defense Civilian Personnel Data System
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DJMS	Defense Joint Military Pay System
FACNET	Federal Acquisition Computer Network
ISSO	Information System Security Officer
MAFR	Merged Accountability and Fund Reporting
NIST	National Institute of Standards and Technology

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

January 22, 1999

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)

SUBJECT: Summary of Audit Results--DoD Information Assurance Challenges (Report No. 99-069)

This summary report is provided for your information and use. Because the report contains no findings or recommendations, no written comments were required, and none were received.

Questions on the report should be directed to Ms. Cecelia A. Miggins at (703) 604-9046 (DSN 664-9046) or Ms. Mary Lu Ugone at (703) 604-9049 (DSN 664-9049). See Appendix D for the report distribution. The contributing team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-069
(Project No. 8AS-6013.01)

January 22, 1999

Summary of Audit Results--DoD Information Assurance Challenges

Executive Summary

Introduction. The DoD Annual Statements of Assurance for FYs 1995 through 1998 identified a material management control weakness in the area of information systems security. Audits have been an important tool in identifying that weakness. In February 1997, the General Accounting Office designated information security as a high-risk area throughout the Federal Government, because weaknesses in information security, in the face of the growing threat, could cause critical Government operations to be highly vulnerable to waste, fraud, abuse, and mismanagement. This report summarizes 75 reports pertaining to DoD organizations or functions and their information assurance efforts.

Objective. The objective of this report is to summarize DoD information assurance weaknesses identified in 75 General Accounting Office and DoD internal audit reports issued from January 1, 1995, through November 30, 1998.

Results. Information assurance problems were identified within the following areas:

- access control (59 reports),
- audit trails (30 reports),
- policies and procedures (57 reports),
- certification and accreditation (22 reports),
- training (29 reports),
- contingency planning (10 reports),
- separation of duties (18 reports),
- management accountability (32 reports),
- physical security (8 reports),
- data aggregation (2 reports),
- resources (7 reports),
- program management (41 reports),
- architecture (10 reports), and
- risk analysis (18 reports).

The results support the need for a sustained effort by DoD managers to improve the Department's information assurance posture.

Table of Contents

Background

The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [ASD(C3I)] is the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for C3I, information management, information operations and other functions. In exercise of these responsibilities, the ASD(C3I) shall serve as the DoD Chief Information Officer (CIO) and senior information security official.

The DoD Annual Statements of Assurance for FYs 1995 through 1998 identified a material management control weakness in the area of information systems security. The 1990's brought a significant increase in computer system intrusions within DoD, which highlighted the vulnerability of information systems to attack. In February 1997, the General Accounting Office designated information security as a high-risk area because weaknesses in information security could cause critical Government operations to be highly vulnerable to waste, fraud, abuse, and mismanagement.

DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, updated and established policy for the safeguarding of classified, sensitive unclassified, and unclassified information processed in automated information systems. The directive provides mandatory, minimum automated information system security requirements. The directive defines "assurance" as the following:

> a measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. If the security features of an AIS are relied on to protect classified or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during AIS operation.

Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 8, 1996, (Circular A-130, Appendix III) lists safeguards for unclassified information. Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Required controls include adequate training, access controls, separation of duties, continuity of support (contingency planning), and periodic review of security controls.

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Report "A Management Process for a Defense-Wide Information Assurance Program," November 1997. The Defense Planning Guidance for FYs 1999 through 2003 required that a new information assurance management process be developed for review and approval by the Deputy Secretary of Defense. This report addresses that requirement and also responds to issues set forth in other DoD studies, which are discussed below.

The report states that the growth in DoD networked information systems offers adversaries targets that, when successfully attacked, can impact vital operations by making essential information or information systems unavailable or can compromise the integrity and confidentiality of critical information. To respond effectively, the report recommended that DoD confront the following two critical and interrelated issues: proliferation of shared or common-user networks across DoD increases the complexity of managing information assurance, and decentralized information assurance management processes are incapable of dealing with the new shared-risk environment. The report states that because DoD did not yet adequately address those critical issues, some information assurance activities across DoD are uneven, unverifiable, and only minimally effective. Currently, DoD lacks the following:

- an effective strategic planning process to identify information assurance requirements on a department-wide basis,
- an integrated process for ensuring that information assurance requirements are programmed and executed in accordance with DoD priorities,
- full visibility of how effectively information assurance resources are being spent,
- appropriate metrics for determining where and how DoD information assurance investments are enhancing the protection and defense of its information systems, and
- an effective process for routinely assessing the operational readiness of DoD information systems and networks.

The report states that at least eight studies addressing DoD information assurance needs have been conducted since 1996. The report builds on the recommendations in some of those studies. Despite all of those efforts, DoD is only beginning to adapt its culture, processes, strategies, and programs to address the information assurance challenges that it faces today. The report makes four key recommendations:

- designate the DoD CIO, working through an expanded DoD CIO Council, as responsible for overseeing DoD development and implementation of an integrated Defense-wide information assurance program;
- institute an integrated information assurance planning process that does the following:
    - promulgates department-wide information assurance goals and objectives and an effective strategy for their achievement;
    - supports decisionmaking for information assurance investment within the Planning, Programming, and Budgeting System; and
    - responds rapidly to emerging information assurance requirements identified in information assurance threat and operational readiness assessments and requirements;

- establish a Defense-wide information assurance program within the DoD resource management structure to ensure that the operational requirements of an effective Defense-wide information assurance program are met; and
- establish information assurance performance measures based on effective, measurable operational readiness criteria.

The report also identifies specific implementing recommendations for each of the four key recommendations.

The report concludes that DoD fully recognized the scope and complexity of the information assurance challenges confronting it. The DoD information assurance challenge lies in integrating its efforts and programs to ensure its ability to gain and maintain information superiority across the spectrum of its diverse missions. Accordingly, the situation requires the creation of a single Defense Information Assurance Program that enables effective DoD CIO oversight of the DoD information assurance operations and resources.

President's Commission on Critical Infrastructure Protection Report, "Critical Foundations Protecting America's Infrastructures," October 1997. The Commission studied the vulnerabilities of the computer dependent systems that underpin modern society and proposed a strategy to protect them. The Commission determined that, even though the U.S. critical infrastructures are the best in the world, they are increasingly dependent on information and communications systems that criss-cross the nation and span the globe. Those infrastructures have substantial vulnerabilities and some have already been exploited. As part of its proposed strategy to protect the infrastructures, the Commission recommended that the President appoint lead agencies to take the initiative to bring together the owners and operators of various infrastructure sectors to create a means for sharing information that is acceptable to all participants. The DoD and the Department of Commerce were proposed as joint leads for the information and communications sector. The information and communications infrastructure consists of the public telecommunications network, the Internet, and the many millions of computers in home, commercial, academic, and Government use. In addition to the disruption of information and communications, there is also the possibility that someone will be able to mount an attack against other infrastructures by exploiting their dependence on computers and telecommunications.

The DoD examined infrastructure vulnerabilities using cyber tools during a joint exercise, Eligible Receiver 1997. A "Red Team" used hacker techniques available on the Internet. Even with no insider information and constrained by U.S. law, the team penetrated many networks and gained system administrator-level privileges in some.

The report recommended that lead agencies promote the development of information sharing, take a leadership and coordinating role with the private sector, and seek appropriate legislation that allows for infrastructure assurance. The report made many recommendations for establishing the Government/private partnership; structuring and building the partnership; and emphasizing the importance of awareness and education, leadership, legal initiatives, research and development, and implementation strategy.

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Report "Improving Information Assurance: A General and Comprehensive Approach to an Integrated IA [Information Assurance] Program for the Department of Defense," March 1997. Program Decision Memorandum II, October 9, 1996, requires the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to provide the Deputy Secretary of Defense an assessment of the Services' and Defense agencies' information assurance programs, a comparison of information assurance plans with programmed resources, and an evaluation of projected program performance. Program Decision Memorandum II also requires the Task Force to provide recommendations for ensuring a well-managed, comprehensive, and balanced Defense-wide information assurance program designed to protect the Defense information infrastructure end-to-end and to effectively detect and react to attacks that do occur.

The report presents the results of the Task Force on the general assessment of DoD information assurance posture and a detailed approach to achieving an integrated information assurance program. The Task Force attempted to obtain data necessary to conduct a detailed assessment. However, data that would support an analysis of DoD information technology investments and their impact on DoD overall information assurance posture was not fully visible or readily attainable. System configuration and personnel data needed to perform an accurate assessment of the DoD information assurance posture are not routinely collected and are not readily available. The report emphasizes that the rapidly changing internetworked and interdependent information environment in which DoD must operate has given rise to the urgent need to transform information assurance from an acquisition activity to an operational imperative. The report acknowledges the benefit of ongoing information assurance initiatives and stresses that DoD must maintain and build upon the initiatives and the momentum that they have created. The report contains explicit goals for the DoD information assurance vision, a supporting process-oriented strategy for program integration, and a comprehensive set of information assurance program components with accompanying action plans.

The Task Force recommended that the report be considered the initial version of a series of plans that must be developed over time. The Service and Defense agency plans should be coordinated across DoD to ensure that, as a composite, the collective plans represent the best information assurance return on investment for DoD. The report "A Management Process for a Defense-Wide Information Assurance Program," November 1997, further addresses the concept of an integrated program.

Defense Science Board Task Force Report, "Information Warfare-Defense," November 1996. The report states that the U.S. national security posture was becoming increasingly dependent on U.S. and international infrastructures. Commercial services from the national information infrastructure provided the vast majority of the telecommunications portion of the Defense information infrastructure. Information infrastructures are vulnerable to attack. Attackers can hide in the mesh of inter-netted systems and often use previously conquered systems to launch attacks. The lack of geographical, spatial, and political boundaries offers further anonymity and legal and regulatory arbitrage. The DoD needed to be concerned about ensured

operation of the critical functions and availability of information necessary to fulfill its missions. The supporting infrastructure, especially its critical portions, needed to be defended. The report concludes that DoD must take extraordinary action to confront the challenges of defending the nation's facilities, information, information systems, and networks against possible information warfare attacks.

The report made more than 60 recommendations and designated the following 13 as key recommendations:

- designate an accountable information warfare focal point,
- organize for information warfare,
- increase awareness,
- assess infrastructure dependencies and vulnerabilities,
- define threat conditions and responses,
- assess information warfare-defense readiness,
- "raise the bar" with high payoff and low-cost items,
- establish a minimum essential information infrastructure,
- focus security research and development,
- staff for success,
- resolve the legal issues,
- participate fully in critical infrastructure protection, and
- provide the resources.

The Chairman, Defense Science Board Task Force on Information Warfare, noted that it was the third consecutive year that a Defense Science Board Summer Study or Task Force had made similar recommendations to better prepare DoD for the challenges of information warfare. See the summary of Report No. NSIAD-98-132R, "DoD's Information Assurance Efforts," June 1998 (Appendix C), for a summary of actions that DoD took to implement the recommendations in the report.

Objective

The objective of this report is to summarize information assurance findings in reports issued by the General Accounting Office; Office of the Inspector General, DoD; Army Audit Agency; Naval Audit Service; and Air Force Audit Agency from January 1, 1995, through November 30, 1998. See Appendix A for a discussion of the scope and methodology. Appendix B provides a matrix identifying which weaknesses were addressed in each of the 75 audit reports. Appendix C contains a summary of each report and the corrective actions taken.

Information Assurance Challenges

General Observations. Based on our analysis of 75 audit reports, we concluded that findings related to information assurance weaknesses fell into 14 categories. Each of those weakness categories is discussed in this section of this summary report. Because audit coverage was much more intensive in the Army, Air Force, and certain Defense agencies, the disproportionate number of reports related to those organizations does not mean that weaknesses are more prevalent in their systems than in those managed by the Navy and other DoD Components.

Access Control. DoD Directive 5200.28 requires automated information systems to have an access control policy in place, including features, procedures, or both, to enforce the access control policy.

Fifty-nine reports discuss conditions related to access control weaknesses. Recommendations for access control improvement were made to various components, including the Army, Navy, Air Force, Defense Information Systems Agency, Defense Finance and Accounting Service, and Defense Investigative Service.

Audit Trails. Audit trails are necessary to detect unauthorized access, modification, or destruction of sensitive computer data and programs. DoD Directive 5200.28 states that the information system security officer must ensure periodic review of audit trails.

Thirty reports address conditions for which audit trails were insufficient or did not exist. The reports are addressed to a range of DoD Components, including the Defense Megacenter-Denver and the Defense Joint Military Pay Systems. Recommendations for improvements were made to various components, including the Army, the Air Force, the Defense Investigative Service, and the Defense Information Systems Agency.

Policies and Procedures. Comprehensive policies and procedures are necessary to provide adequate security guidance to system administrators and users. DoD Standard 5200.28, "Department of Defense Trusted Computer System Evaluation Criteria," December 1985, contains policy guidelines for computer system security requirements. It also states that for controlled access protection (class C2 security), a trusted facility manual addressed to the automatic data processing system administrator should present cautions about functions and privileges that should be controlled when running a secure facility. The trusted facility manual should give procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event. Inadequate security guidance and implementation may compromise computer security and allow for unauthorized access, modification, or destruction of sensitive computer data and programs, as well as theft or destruction of computer equipment.

Fifty-seven reports discuss conditions in which policies and procedures were either inadequate or did not exist. The reports are addressed to DoD Components, including the DoD overall, the Army, the Defense Finance and Accounting Service, and the Defense Information Systems Agency. Recommendations to improve policy and procedures were made to various components, including the Army, the Air Force, the Defense Finance and Accounting Service, the Defense Investigative Service, and the Defense Retirement Trust Fund.

Certification and Accreditation. DoD Directive 5200.28 requires that automated information systems that process or handle classified information, sensitive unclassified information, or both, and that require at least class C2 security implement certain security features. If a risk assessment described in the directive requires security above class C2, a designated approving authority is responsible for the accreditation of an automated information system to ensure that adequate security measures are in place. A certification plan, a risk analysis, an evaluation of security safeguards, and a certification report must support the accreditation.

Twenty-two reports describe conditions related to certification and accreditation. The recommendations were addressed to various DoD Components, including the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), the Army, the Air Force, the Defense Information Systems Agency, and the Civilian Personnel Management Service.

Training. Adequate training is necessary for system administrators and users to understand their roles and responsibilities in implementing and maintaining adequate system security. Circular A-130, Appendix III, states that before individuals have access to a major application, they should receive specialized training focused on their responsibilities and the application rules. The training may be in addition to the training required for system access. Such training may vary from a notification at the time of access to formal training for employees working with high-risk applications.

Twenty-nine reports address conditions related to inadequate security training. In addition, the General Accounting Office identified a DoD-wide deficiency in the area of training. For example, Army Audit Agency Report No. AA 99-5, "Information Systems Security Program Phase II Follow-On Validation," October 15, 1998, states that the information systems of the Army may be vulnerable to attack for several reasons, including training programs that did not reach all information systems security personnel and that did not provide the technical training necessary for personnel to protect information systems from unauthorized access, malicious attacks, exploitation, and denial of service.

Contingency Planning. Circular A-130, Appendix III, states that a system should have procedures in place to ensure continuity of operations and a formal security plan, including contingency plans, for each major application. The contingency plan should establish capabilities to perform the supported functions in the event of failure of automated support.

Ten reports describe conditions related to weaknesses in contingency planning. Recommendations to improve contingency planning were made to various DoD Components, including the Navy; the Defense Information Systems Agency; and the Military Retirement Trust Fund managers.

Separation of Duties. Office of Management and Budget Circular No. A-123, "Management Accountability and Control," June 21, 1995, states that key duties and responsibilities in authorizing, processing, recording, and reviewing official agency transactions should be separated among individuals.

Eighteen reports address conditions related to separation of duties. For example, Office of the Inspector General, DoD, Report No. 98-082, "Information Assurance of the Defense Civilian Personnel Data System," February 23, 1998, states that the acquisition program manager also had security certification and accreditation responsibilities. Without independent oversight, the acquisition program manager could define the Defense Civilian Personnel Data System security safeguards, design them into the system, assess the adequacy of the safeguards, modify the safeguards, approve the safeguards, and accredit the Defense Civilian Personnel Data System for operations. As a result, the Defense Civilian Personnel Data System had high risks for unauthorized system access, intentional and unintentional alteration and destruction of data, and denial of service to authorized users.

Management Accountability. Circular A-130, Appendix III, states that a Federal agency should assign the responsibility for security of an information system to an individual knowledgeable in the information technology used in the system and in providing security for such technology. More generally, Circular No. A-123 defines management accountability as the expectation that managers are responsible for the quality and timeliness of program performance, increasing productivity, controlling costs and mitigating adverse aspects of agency operations, and ensuring that programs are managed with integrity and in compliance with applicable law.

Thirty-two reports discuss conditions related to accountability weaknesses. For example, Office of the Inspector General, DoD, Report No. PO 97-049, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems," September 25, 1997, concludes that a lack of accountability for information systems security management controls contributed to the inadequate security safeguards for DoD automated information systems. As a result, the reliability and integrity of automated information systems critical to support the readiness of U.S. forces could be compromised, and vital day-to-day operations relying on automated information systems could be in jeopardy. The report states that implementation of the recommendations in the report would help the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in developing an approach to correct the systemic control weaknesses of DoD automated information systems.

Physical Security. DoD Directive 5200.28 states that physical security (such as guards or locked doors) is one means to safeguard information and automated information system resources against the possibilities of sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons.

Eight reports describe conditions related to physical security. The reports are addressed to a very wide range of DoD Components, including the Army, the Air Force, the Defense Finance and Accounting Service, and the Defense Investigative Service.

Data Aggregation. DoD Regulation 5200.1-R, "Information Security Program," January 1997, established the DoD Information Security Program to promote proper and effective classification, protection, and downgrading of official information requiring protection in the interest of the national security.

In two reports, Defense organizations had a reported weakness related to data aggregation. Users could access various unclassified information systems and obtain data that, if combined, could become classified. For example, Air Force Audit Agency Project No. 97066029, "Global Combat Support System-Air Force," November 19, 1997, states that the Global Combat Support System-Air Force security plan did not include specific security requirements or procedures to prevent data aggregation. The Global Combat Support System-Air Force would provide critical data to support command and control functions in peacetime and wartime.

Resources. The Paperwork Reduction Act of 1995 emphasizes the need for agencies to acquire and apply resources to effectively support the accomplishment of agency missions. The Clinger-Cohen Act of 1996 repeated that theme and provided more detailed requirements. The costs to an organization for computer security policy development and implementation would depend upon what was needed to achieve a level of risk acceptable to management. Also, defined budgets give an organization the ability to plan and set goals for information security.

Seven reports discuss conditions related to resources. For example, General Accounting Office Report No. AIMD-98-257, "Defense Information Superiority Progress Made, but Significant Challenges Remain," August 1998, states that past architecture efforts by DoD were not successful in part because DoD lacked centralized or joint managerial and funding control over individual Service priorities, which often took precedence. Recommendations were made to several DoD Components, including the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), the Army, and the Air Force.

Program Management. Security program management is a central factor affecting an organization's ability to protect its information resources and the program operations that the resources support. The ability to elevate significant security concerns to higher management levels helps ensure thorough understanding of risks and careful consideration of decisions related to risks before final decisions were made.

Forty-one reports address conditions related to program management. The reports are addressed to a very wide range of DoD Components, including the Army, the Navy, the Air Force, the Defense Information Systems Agency, and the Defense Finance and Accounting Service.

Architecture. The DoD Goal Security Architecture is a generic architectural framework for developing mission-specific security architectures. The standards mandated for the development and acquisition of application software are DoD Standard 5200.28 and NCSC-TG-021, Version 1, "Trusted Database Management System Interpretation," April 1991.

Ten reports discuss conditions related to architecture. For example, Office of the Inspector General, DoD, Report No. 98-024, "Security Controls Over Systems Serving the DoD Personnel Security Program," November 19, 1997, states that the Defense Investigative Service implemented its network using an open architecture, which left critical network components vulnerable to internal and external attacks. Because of physical security weaknesses, unauthorized personnel could have entered the center and obtained access to all Defense Investigative Service automated data, which included sensitive information, or could have stolen equipment. Other DoD organizations with weaknesses related to system architecture included the Office of the Secretary of Defense, the Defense Information Systems Agency, the Army, and the Air Force.

Risk Analysis. Understanding the risks associated with information security is the starting point of the risk management cycle. Identifying and assessing information security risks in terms of the impact on operations is an essential step in determining the controls that are needed and the level of resources to spend on controls. Circular A-130, Appendix III, states that the need to determine adequate security requires the use of a risk-based approach. It states that the risk assessment approach should include a consideration of the following major factors of risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.

Eighteen reports address conditions related to risk analysis. For example, Office of the Inspector General, DoD, Report No. 98-143, "Information Assurance for the Defense Civilian Personnel Data System – Washington Headquarters Services," June 3, 1998, states that because Washington Headquarters Services had not performed a risk analysis, it did not know what its risks and vulnerabilities were, and it did not have assurance that its system was secure in accordance with DoD regulations. As a result, Washington Headquarters Services could not ensure the confidentiality, integrity, and availability of more than 10,000 personnel records. Recommendations related to risk analysis were made to various components, including the Office of Management and Budget, the DoD overall, the Army, and the Air Force.

Information Assurance Guidance

The following three publications give Government organizations guidance on both the security management and the security implementation perspectives.

Report No. AIMD-98-68, "Executive Guide Information Security Management Learning From Leading Organizations," May 1998. To gain a broader understanding of how information security programs can be

successfully implemented, the General Accounting Office studied management practices of eight non-Federal organizations recognized as having strong information security programs. The study focused on the management framework because previous audit work identified security management as an underlying problem at Federal agencies, including DoD. The need to protect sensitive and critical data is recognized in various laws and other guidance, including the following:

- the Privacy Act of 1974;
- the Paperwork Reduction Act of 1995;
- the Computer Security Act of 1987;
- the Clinger-Cohen Act of 1996;
- the Federal Managers' Financial Integrity Act of 1996;
- the Chief Financial Officers Act of 1990;
- Circular A-130, Appendix III, February 1996;
- National Institute of Standards and Technology (NIST) Special Publication 800-12, "An Introduction to Computer Security: the NIST Handbook," October 1995; and
- NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," September 1996.

The General Accounting Office discussed its findings at the non-Federal organizations with numerous Federal officials to determine the applicability of the non-Federal practices to Federal agencies. The key to the effectiveness of the leading organizations is applying 16 practices related to five fundamental risk management principles. The principles are as follows:

- assess risk and determine needs,
- establish a central management focal point,
- implement appropriate policies and related controls,
- promote awareness, and
- monitor and evaluate policy and control effectiveness.

The report discusses the 16 practices in detail. The report concludes that an agency can strengthen its security posture, facilitate future system and process improvement efforts, and more confidently take advantage of technology advances by instituting a management framework as a cycle of activity.

NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," September 1996. The publication provides a baseline that organizations can use to establish and review their information technology security programs. The publication is a reference document to be used to gain an understanding of the basic security requirements that information technology systems should contain. The security implementation begins with generally accepted system security principles and continues with common practices that are used in securing information systems.

The principles are expressed at a high level for the following broad areas: accountability, cost-effectiveness, and integration. Practices are guidance on the types of controls, objectives, and procedures that comprise an effective information technology security program. The following eight principles provide an anchor on which the Federal community should base its information technology security programs. The principles are as follows:

- computer security supports the mission of the organization,
- computer security is an integral element of sound management,
- computer security should be cost-effective,
- computer security responsibilities and accountability should be made explicit,
- computer security requires a comprehensive and integrated approach,
- computer security should be periodically reassessed,
- computer security is constrained by societal factors, and
- systems owners have security responsibilities outside their own organizations.

The publication discusses 14 common information technology security practices. The publication serves as a companion to the NIST Special Publication 800-12, which is discussed as follows. The publication is available electronically at http://csrc.nist.gov/nistpubs.

NIST Special Publication 800-12, "An Introduction to Computer Security: the NIST Handbook," October 1995. The handbook provides assistance in securing computer-based resources, including hardware, software, and information, by explaining important concepts, cost considerations, and interrelationships of security controls. It illustrates the benefits of security controls, the major techniques or approaches for each control, and important related considerations. The handbook gives an introduction and overview of the elements of computer security, roles and responsibilities, and common threats.

The handbook then discusses management controls, operational controls, and technical controls. The management controls section discusses techniques and concerns that are used to manage the organization's computer security program and risk. Operational controls are security controls that people implement and execute. Technical controls are the security controls that the computer system executes. The handbook discusses interdependencies and gives references for additional guidance. The handbook is available electronically at http://csrc.nist.gov/nistpubs.

Other NIST Special Publications available include the following:

Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," December 1998, available electronically at http://csrc.nist.gov/nistpubs;

Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," March 1998, available electronically at http://csrc.nist.gov/nistpubs; and

Special Publication 800-4, "Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials," March 1992, available electronically at http://csrc.nist.gov/nistpubs.

Conclusion

Weaknesses in the area of DoD information assurance are a significant problem and warrant continued management attention. We plan to continue auditing selected information assurance aspects of DoD information systems or capabilities that use electronic technologies. We will focus on the need to build in information assurance controls during development or modernization efforts. Given audit resource constraints and the nature of the problem, however, all DoD automated system owners and users must self-assess their controls more rigorously than many have done in the past.

Appendix A. Process

Scope

This report summarizes Defense organizations' information assurance weaknesses identified in 75 audit reports that the General Accounting Office; the Office of the Inspector General, DoD; the Army Audit Agency; the Naval Audit Service; and the Air Force Audit Agency issued from January 1, 1995, to November 30, 1998. In addition, we summarized management's corrective actions.

Government Performance and Results Act

DoD-Wide Corporate-Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, the Department of Defense has established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting the objectives. This report pertains to achievement of the following objective and goal.

- **Objective:** Prepare now for an uncertain future. **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. **(DoD-3)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals:

- **Information Management Functional Area. Objective:** Ensure DoD's vital information resources are secure and protected. **Goal:** Build information assurance framework. **(ITM-4.1)**
- **Information Management Functional Area. Objective:** Ensure DoD's vital information resources are secure and protected. **Goal:** Build information assurance architecture and supporting services. **(ITM-4.2)**
- **Information Management Functional Area. Objective:** Ensure DoD's vital information resources are secure and protected. **Goal:** Assess information assurance posture of DoD operational systems. **(ITM-4.4)**

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the Department of Defense. This report provides coverage of the Information Management and Technology high-risk area.

Appendix B. Matrix of Information Assurance Weaknesses

Report No.	Access Control	Policy Proced.	Training	Sep. Duty	Physical Security	Resrcs.	Arch.
General Accounting Office							
AIMD-98-257		X				X	X
AIMD-98-92	X	X	X	X			
NSIAD-98-132R		X					X
OCG-98-1R		X					
AIMD-97-128	X	X		X	X		
HR-97-30	X	X	X			X	
HR-97-9	X		X				
AIMD-96-144	X	X	X	X	X		
AIMD-96-110			X				
AIMD-96-84	X	X	X				
AIMD-95-73	X						
Inspector General, DoD							
98-143		X	X				
98-127		X	X				
98-082	X			X			

Report No.	App. Proc.	Access Control	Audit Trails	Policy Proced.	Cert. Accred.	Training	CP Plan	Sep. Duty	Audit	Physical Security	Tel. Secur.	Resrcs.	Prog. Sec. Mgmt.	Arch.	Risk Analysis
98-041				X				X							
98-024		X		X						X				X	
98-012		X													
98-007		X		X											
PO 97-049		X		X		X									
97-216		X		X											
97-203		X		X											
PO 97-024				X								X			
96-214		X		X											
96-179		X		X										X	
96-175		X		X		X		X							
96-172				X											
96-124		X		X		X		X							
96-053		X		X											
95-264		X		X											
95-263		X		X											

Report No.	Access Control	Policy Proced.	Training	Sep. Duty	Physical Security	Resrcs.	Arch.
95-259	X	X	X				
Army Audits							
AA 99-5	X	X	X			X	
AA 98-265	X					X	
AA 98-170	X	X					
AA 98-123	X	X	X				
AA 98-10		X	X				
AA 98-32	X	X	X				
AA 98-28	X				X		
AA 98-9	X		X				
AA 98-2	X	X					
AA 97-306	X	X					
AA 97-293	X						
AA 97-767			X			X	
AA 97-214	X	X	X				
AA 97-53	X	X					

Report No.	Access Control	Policy Proced.	Training	Sep. Duty	Physical Security	Resrcs.	Arch.
AA 96-28	X	X	X				X
NR 95-428	X						
SR 95-722	X			X			X
Naval Audit							
059-95	X	X	X		X		
Air Force Audit							
98054006	X	X				X	
98066011	X	X					
97066028		X	X				
97066030	X						
97066033	X						
97068016	X	X	X				
97066029		X					
97066024		X					
96068016	X						X
96066029	X	X	X	X			X

Report No.	Access Control	Policy Proced.	Training	Sep. Duty	Physical Security	Resrcs.	Arch.
97054014	X	X		X			
96054027			X				
96066009	X	X					
96066012	X	X	X				X
96066010	X	X		X			
96054010	X	X		X			
95066023	X	X		X			
95066008	X			X			
95066019	X	X	X	X			
95066021	X	X					
95066003	X	X					
95066007	X			X			X
94066013		X					
94066006	X	X	X	X	X		
93058001	X	X	X	X	X		
94066003	X	X			X		

Acct.	Management Accountability
App. C Page	Appendix C Page Reference
Arch.	Architecture
ASD (C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Cert. Accred.	Certification and Accreditation
Cont. Plan	Contingency Planning
Data Aggr.	Data Aggregation
DIAP	Defense-Wide Information Assurance Program
DSB	Defense Science Board
IA	Information Assurance
Policy Proced.	Policies and Procedures
Program Mgmt.	Program Management
Resrcs.	Resources
Sep. Duty	Separation of Duties

Appendix C. Synopsis of Information Assurance Issues

General Accounting Office

Report No. AIMD-98-257, "Defense Information Superiority Progress Made, but Significant Challenges Remain," August 1998. The DoD Joint Vision 2010 conceptual framework for warfighting identifies information superiority as an essential element for success over the enemy. Achieving information superiority is complex because it involves thousands of decentralized command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR) systems and information networks managed by many different offices of the Secretary of Defense, Joint Chiefs of Staff, Services, unified commands, and Defense agencies throughout DoD. Two of the key activities for DoD to achieve information superiority are development of a department-wide C^4ISR information systems architecture to guide and control the development and maintenance of many related systems and implementation of a department-wide information assurance program to protect and defend its C^4ISR systems from intrusion and attack. The report states that the architecture is critical. At the technical level, the architecture provides rules and standards for hardware, software, communication, data, security, and performance characteristics. Without an overall architecture, DoD would have difficulty identifying, establishing, and prioritizing information and information links within DoD; the communications processes and technical standards; the systems and interoperability for timely information transfer; and measures needed to protect the systems, information, and supporting infrastructure. The report found that the past architecture efforts were not successful because DoD lacked centralized or joint managerial and funding control over individual Service priorities, which often took precedence, and DoD organizations have not agreed on the architecture. The information assurance program remains incomplete, and the DoD information assurance efforts are moving forward without a completed and approved C^4ISR architecture. The report further states that the Chairman of the Joint Chiefs of Staff cited the need for a management structure to enforce compliance with the architecture. The report recommended the following of DoD:

- establish milestones for completing the C^4ISR architecture and information assurance program and
- ensure that the C^4ISR management structure has sufficient authority and is effective in enforcing compliance with the C^4ISR architecture.

The report states that DoD should consider incorporating architecture compliance into its planning, programming, and budgeting process and C^4ISR systems funding decisions.

Management generally concurred with the recommendations and provided details on plans to complete development and implementation of the architecture

and information assurance program and described the oversight organizations and processes that it will rely on to achieve compliance with the C4ISR architecture. Management did not provide details of how or when the systems architecture would be completed. Finally, DoD stated that it provides C4ISR architecture progress information to Congress through documents such as the congressional justification books. The report states that the documents to which DoD referred do not provide a comprehensive overview of the DoD C4ISR architecture progress within the context of the architecture and information superiority goals. The DoD officials agreed that a department-wide perspective is not available and agreed that such information may be useful to Congress and DoD in overseeing C4ISR investments.

Report No. AIMD-98-92, "Information Security Serious Weaknesses Place Critical Federal Operations and Assets at Risk," September 1998. The report evaluates the effectiveness of Federal agencies' information security practices and efforts to centrally oversee and manage Federal information security. The increasing reliance on interconnected systems and electronic data increased the risks of fraud, inappropriate disclosure of sensitive data, and disruption of critical operations and services. Evaluations of computer security present a disturbing picture of Federal agencies, including DoD, and their lack of success in protecting their assets from fraud and misuse, sensitive information from inappropriate disclosure, and critical operations from disruption. The report states that the weaknesses at DoD increase the vulnerability of military operations that support the DoD warfighting capability. The attacks on DoD computer systems were a serious and growing threat, and only a small portion were actually detected and reported. The report further states that according to DoD officials, attackers obtained, stole, modified, and destroyed both data and software; installed unwanted files and "back doors," which circumvent normal system protection and allow future unauthorized access; and shut down and crashed entire systems and networks, denying service to users. Numerous DoD functions had been adversely affected, including weapons, supercomputer research, logistics, finance, procurement, personnel, management military health, and payroll. The attacks continued to be a problem. Previous reviews identified a broad array of control weaknesses, including lack of segregation of duties, weak access controls, lack of an adequate comprehensive disaster recovery plan, weak authentication controls, and other weaknesses too sensitive to be reported publicly. The report made no further recommendations. The report summarizes General Accounting Office Report No. AIMD-98-68, "Information Security Management: Learning From Leading Organizations," May 1998, and states that agency management is ultimately responsible for ensuring that information security controls are appropriately selected and effectively implemented on an ongoing basis. Finally, the report states that agencies needed to provide more active oversight for previous recommendations and agency security programs, including a security plan, screening and training of users, assessing risk, disaster and contingency planning, and periodic review of security safeguards as required by Circular A-130, Appendix III.

Report No. NSIAD-98-132R, "DoD's Information Assurance Efforts," June 1998. The report discusses DoD actions to implement the recommendations from the Defense Science Board Task Force Report, "Information Warfare-Defense," November 1996; the development of the DoD information

assurance management process; and DoD adoption of a new information assurance certification and accreditation process. The report states that DoD organizations undertook a variety of efforts to establish information assurance. However, the effectiveness of the new initiatives remained to be demonstrated. The report states that several of the task force recommendations did not fall entirely within the DoD scope of operations, some of the task force recommendations were considered and rejected, DoD had certain efforts underway to address some of the task force recommendations, and DoD would address some of the recommendations through implementation of recently adopted plans and processes. The report concludes that DoD information assurance needs were not being met in certain key areas, despite the effort by various DoD organizations. The DoD had taken steps to develop and implement a DoD-wide information assurance program. However, the DoD information assurance efforts were moving forward without a completed and approved C^{4}ISR architecture. The DoD adopted a new Information Technology Security Certification and Accreditation Process, Instruction 5200.40, December 1997, as a standard DoD-wide approach to protecting and securing the Defense information infrastructure. Successful operation of the new certification and accreditation process remained to be seen because the process dispersed certification and accreditation responsibilities among organizations and systems. Also, the process permitted dispersed risk acceptance, which means that the most vulnerable system sets the risk level for other interconnected systems.

Report No. OCG-98-1R, "Federal Management," January 1998. The report states that information security was a high-risk area that affected virtually all aspects of Government operations. The DoD long-standing management weaknesses were the underlying cause of the DoD high-risk areas. Those underlying factors include cultural barriers and Service parochialism, lack of incentives for seeking and implementing change, deficient management data, lack of clear results-oriented goals and performance measures, and inadequate management accountability and follow through. To effectively address the underlying causes would require congressional support and a commitment by senior-level DoD managers to a multilevel strategy that implements recommendations to correct specific problems and develops and implements a strategic plan that addressed actions for eliminating the high-risk area. In developing the strategic plan, DoD was to comply with the Chief Financial Officers Act, the Government Performance and Results Act, the Paperwork Reduction Act, and the Clinger-Cohen Act. To help ensure success of the multilevel strategy, top-level management within DoD needs to be held accountable and have the authority and flexibility to achieve the desired results.

Report No. AIMD-97-128, "Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls," September 1997. The DoD Military Retirement Trust Fund records funds to finance DoD liabilities for military retirement and survivor benefit programs. The report is a General Accounting Office sponsored report by the KPMG Peat Marwick accounting firm. The review determined that DoD lacked overall security administration and management governing access to data files. Specifically, the report states that DoD had not adequately implemented security policies and

procedures, controlled the ability of computer programmers to make changes to systems, or controlled access to information on pension fund participants. The report recommended that DoD:

- modify the security program to ensure that data and programs are protected and security requirements comply with regulations;
- implement security features and parameters to ensure that unauthorized access is reduced and audit trails are activated and protected from unauthorized editing;
- implement security policies and procedures to ensure that all authorized users access only necessary facilities and data, user access is periodically reviewed and removed if warranted, and access violations are researched;
- develop and implement a comprehensive change management procedure governing changes to both the applications programs and operating systems;
- design, develop, test, and implement a comprehensive disaster recovery plan; and
- assess and document the year 2000 risk and prepare a contingency plan, if needed.

Management concurred and prepared a corrective action plan addressing the weaknesses cited in the report. The General Accounting Office sponsored a followup report by KPMG Peat Marwick and expected to issue a report on the status of the implementation of the recommendations in the near future.

Report No. HR-97-30, "High-Risk Program Information on Selected High-Risk Areas," May 1997. The General Accounting Office identified information security as a high-risk area that touches virtually every major aspect of Government operations. System interconnectivity, combined with poor security management, resulted in serious, pervasive risks. As an example, the report discusses the attack on the Air Force Rome Laboratory. In the Rome incident, two hackers took control of laboratory support systems for several days, established links to foreign Internet sites, stole tactical and artificial intelligence research data, and successfully attacked systems at other Government facilities. The Air Force caught the hackers. However, the Air Force never conclusively determined what was done with the copied data. The attack cost the Government more than $500,000 at the Rome Laboratory alone. The report states that the General Accounting Office made many recommendations to agencies for improvement, and the agencies had acted on many of the recommendations. However, to help ensure adequate protection of systems and data on a continuing basis, agencies were to address several underlying factors. The factors include insufficient awareness and understanding of information security risks among senior agency officials, poorly designed and implemented security programs that did not adequately monitor controls or proactively address risk, a shortage of personnel with the technical expertise needed to manage controls in today's sophisticated information technology environment, and limited oversight of agency practices at a Government-wide level. The challenge for Congress and managers was to view information-security risk management as an integral element of program

management, to include considering security implications whenever computer and telecommunications technology is used to support program operations, weighing the potential costs and benefits, determining the acceptable level of risk, and providing adequate resources to monitor controls and keep risks at an acceptable level. The report states that in light of the increasing importance of information security and the pattern of widespread problems that had emerged, the Government, including DoD, needed stronger central leadership.

Report No. HR-97-9, "Information Management and Technology," February 1997. The Federal Government's dependence on computer systems, networks, and electronic records to carry out its work continued to accelerate. The General Accounting Office designated information security as a high-risk area because despite the sensitivity and criticality of the information systems, they were not being adequately protected. The report states that greater use of interconnected systems promised significant benefits. However, such systems were much more vulnerable to anonymous intruders, who could manipulate data to commit fraud, obtain sensitive information, severely disrupt operations, and put billions of dollars' worth of assets and vast amounts of sensitive data at risk. The DoD may have experienced 250,000 attacks in 1995, and only a small percentage were detected. The report states that General Accounting Office reports contain dozens of recommendations to individual agencies for improvement. However, several underlying factors needed to be addressed to help ensure that systems and data were adequately protected. The factors include insufficient awareness and understanding of information security risks among senior agency officials, poorly designed and implemented security programs that did not adequately monitor controls or proactively address risk, a shortage of personnel with the technical expertise needed to manage controls in a sophisticated information technology environment, and limited oversight of agency practices at a Government-wide level. The report concludes that, in light of the increasing importance of information security and the pattern of widespread problems that has emerged, stronger central leadership is needed. The Office of Management and Budget needed to play a more proactive role in promoting awareness and in monitoring agency practices and was to encourage CIO council members to adopt information security as one of their top priorities and develop a strategic plan for addressing the root causes of agency security problems. The Office of Management and Budget reported that it had begun efforts to improve its oversight of Federal agency information security activities.

Report No. AIMD-96-144, "DoD General Computer Controls Critical Need to Greatly Strengthen Computer Security Program," September 1996. The report addresses the DoD computer security program. The DoD computer security management needed significant improvement and was not effective. Security weaknesses were in access controls, separation of duties, physical and environmental protection, service interruption controls, and program change controls. Overall, DoD general computer control weaknesses impaired its ability to ensure the integrity and reliability of data related to essential operations. Also, DoD did not have adequate general computer controls to protect its computer systems and data from outside hackers, unauthorized DoD employees, or contractor personnel. The computer control weaknesses were identified throughout DoD for several years, but the risk that they present was not effectively mitigated and continued to grow. The computer control

weaknesses could be greatly improved by a stronger DoD-wide computer security management program. The report recommended that the Secretary of Defense:

- assign clear responsibility and accountability within DoD for ensuring successful implementation of the DoD information security program;
- direct the DoD CIO to develop and implement a comprehensive, DoD-wide computer security management program, which includes the following:
  - establishing a risk-based control program to assess computer security in DoD computer systems,
  - developing and implementing effective security policies and related control techniques, and
  - reporting to DoD managers on security issues impacting their information processing systems;
- direct the Deputy Secretary of Defense to ensure that the duties established for the Military Departments' and Defense agencies' CIOs include reporting ongoing computer security efforts and activities to the DoD CIO for review, assessment, and appropriate action to ensure proper coordination and an integrated information technology structure within DoD; and
- direct the DoD CIO to monitor and to periodically report on the status of the actions taken to improve computer security throughout DoD and ensure that the DoD CIO has the necessary authority to ensure that there are adequate computer security controls throughout DoD, including the Military Departments and Defense agencies.

The report also recommended the following:

- that the DoD CIO direct the Director, Defense Information Systems Agency (DISA), to develop and implement a comprehensive computer security program, consistent with the DoD-wide program, to ensure that access to computer facilities is appropriately granted and periodically reviewed; roles and responsibilities of users, information systems security officers, and security managers are clearly defined; and security oversight to monitor, measure, test, and report the effectiveness of computer systems, networks, and process controls is in place;
- that the Director, DISA, and CIOs of the Military Departments and Defense agencies submit their policies and procedures to improve general computer controls to the DoD CIO for review, assessment, and appropriate action to ensure that a comprehensive security approach is operational throughout DoD;
- that the Military Departments' and Defense agencies' CIOs submit plans for coordinating with DISA to improve computer controls to the DoD CIO for review, assessment, and appropriate actions; and

- that the Director, DISA, and the Military Departments' and Defense agencies' CIOs should provide their plans to the DoD CIO for review, assessment, and appropriate action to ensure that computer system security reviews are performed as part of future transfers of computer systems.

The report recommended that the DoD CIO monitor implementation of those plans.

DoD management concurred with all findings and recommendations and stated that it had taken or plans to take corrective actions. Management acknowledged that risk was increasing to the daily operation of DoD information systems. The General Accounting Office was performing a followup audit on DoD implementation of the recommendations. The General Accounting Office planned an exit conference to present the followup findings for the end of December 1998. The exit conference had been postponed until January 1999.

Report No. AIMD-96-110, "Information Security Opportunities for Improved OMB [Office of Management and Budget] Oversight of Agency Practices," September 1996. The report concludes that implementing effective information security programs was primarily the responsibility of managers at individual Federal agencies because they were the most familiar with program risks, and they had the ability to bring resources to bear where they would be most effective. However, the Office of Management and Budget was responsible for overseeing those activities. The report recommended that, to improve its oversight capability, the Office of Management and Budget should accomplish the following:

- advocate and promote the CIO Council adoption of information security as one of its top priorities and develop a strategic plan for increasing awareness of the importance of information security, especially among senior agency executives, and improving information security program management Government-wide;
- proactively monitor the effectiveness of agency security practices;
- develop improved sources of information to monitor compliance with Office of Management and Budget guidance and the effectiveness of agency information security progress; and
- develop a program to increase program examiners' understanding of information security management issues.

Report No. AIMD-96-84, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," May 1996. The report discusses the extent to which DoD computers were being attacked, the potential for damage, and the challenges that DoD faced in securing sensitive information. The report states that attacks on DoD computer systems were a serious and growing threat. At a minimum, the attacks were a multimillion-dollar nuisance to DoD, and at worst, they were a serious threat to national security. Attackers seized control of entire DoD systems, many which support critical functions, such as weapons systems research and development, logistics, and finance. The DoD was acting to address the growing problem, but faced significant challenges in controlling unauthorized access to its

computer systems. The report states that DoD challenges included the following: policies are outdated and inconsistent, users were often unaware of system vulnerabilities and weak security practices, and the majority of system and network administrators were inadequately trained and did not have sufficient time to perform their duties.

The report recommended that the Secretary of Defense accomplish the following:

- ensure sufficient priority, resources, and top-management attention for establishing a more effective information systems security program;
- establish a more effective information systems security program that includes the following:
  - improving security policies and procedures,
  - increasing user awareness and accountability,
  - setting minimum standards for ensuring that system and network security personnel have sufficient time and training to properly do their jobs, and
  - implementing more proactive technical protection and monitoring systems and evaluating DoD incident response capability; and
- assign clear responsibility and accountability throughout DoD for the successful implementation of the security program.

DoD officials agreed with the report's findings and recommendations and stated that the report fairly represents the increasing threat of attacks on DoD computers and networks. The DoD officials believed that a large part of the DoD security problems resulted from poorly designed systems or the use of commercial off-the-shelf computer hardware and software products that had little or no inherent security. Also, management cited recent actions taken to improve security, such as the Defense Information Systems Agency information systems security implementation plan and the Joint Chiefs of Staff instruction on defensive information warfare.

DoD has continued the review and revision of DoD Directive 5200.28. The review began in June 1997, was expected to be ready for release in September 1997, and was later expected for March 1999. The assessment for DoD knowledge requirements for key security responsibilities was to be completed in June 1997. That assessment recommended establishing an integrated process team to address information assurance training with completion in March 1999. The Services initiated programs to employ more intrusion detection software into their systems. Assessment of the DoD incident response capability within the Defense Information Systems Agency and a proposed revision or replacement to DoD Instruction 5215.2, "Computer Security Technical Vulnerability Reporting Program," was scheduled to be ready for review the third quarter of 1999. Finally, DoD stated that the Office of the Secretary of Defense would ensure that more prescriptive practices were mandatory to improve accountability and that the Assistant Secretary of Defense (Command,

Control, Communications, and Intelligence)/CIO would further provide clarity of responsibility and authority for ensuring the security of DoD information systems. However, specific actions were not adequately documented.

Report No. AIMD-95-73, "Financial Management: Control Weaknesses Increase Risk of Improper Navy Civilian Payroll Payments," May 1995. The report states that Defense Finance and Accounting Service civilian payroll operations for the Navy did not properly control access to pay and personnel data and did not maintain effective audit trails. Unless the vulnerabilities were corrected, the civilian payroll accounts consolidation could increase the control weaknesses. The report recommended that DoD assess the level of access needed by each user and develop adequate audit trails to mark all transactions with user identification that cannot be overwritten. Management generally agreed with the recommendations, but expressed concern that the audit did not fully recognize the extenuating circumstances brought about by the rapid civilian pay system consolidation. Management continued granting supervisory access to nonsupervisory personnel and would reduce the access as the accounts became stabilized. Management had also procured, tested, and installed software on all Defense civilian pay system computers to implement audit trails.

Office of the Inspector General, DoD

Report No. 98-143, "Information Assurance for the Defense Civilian Personnel Data System - Washington Headquarters Services," June 3, 1998. The Defense Civilian Personnel Data System (DCPDS) is an automated civilian personnel information system. The audit showed that the Washington Headquarters Services had a security policy, security plan, contingency plan, and system access and physical security controls in place. However, Washington Headquarters Services did not have required information assurance controls in place to conduct a risk analysis, complete a systems security test and evaluation, or obtain assurance that its customer support units had completed a security plan, contingency plan, and system accreditation. Furthermore, the DCPDS and Washington Headquarters Services managers had not coordinated to provide training for DCPDS security personnel. Without adequate information assurance controls, the Washington Headquarters Services could not ensure the confidentiality, integrity, and availability of more than 10,000 personnel records. Management concurred with the recommendations and initiated corrective actions. Washington Headquarters Services management conducted a risk analysis for its organization and developed a security annex to the DCPDS Training Support Plan. Also, management was in the process of conducting a systems test and evaluation of its infrastructure and establishing memorandums of agreement with the customer support units.

Report No. 98-127, "Information Assurance of the Defense Civilian Personnel Data System - Navy," April 29, 1998. The audit evaluated security planning, risk analysis, and security management of DCPDS Navy. The report states that management had taken corrective actions during the audit by developing a security policy and interim authority to operate and by conducting a system security test and evaluation. Management also appointed key security

management positions, established a risk analysis safeguard checklist to identify and define overall system threats and vulnerabilities for the computers that run DCPDS, and initiated ongoing security awareness training in accordance with the Computer Security Act of 1987. However, information assurance for the Human Resources Office Marine Corps Base Hawaii Kaneohe Bay still needed improvement because it did not have an overall security plan and a contingency plan. Further, the DCPDS functional and acquisition managers did not coordinate with the Navy about their respective roles and responsibilities for the DCPDS information assurance program. The report states that without those controls, the Navy could not ensure the confidentiality, integrity, and availability of more than 209,000 Navy and Marine Corps civilian personnel records. The Navy concurred with the recommendations and developed for DCPDS a security plan and a contingency plan that includes a disaster recovery plan.

Report No. 98-082, "Information Assurance of the Defense Civilian Personnel Data System," February 23, 1998. The report states that the DCPDS information assurance program did not have adequate controls in place to safeguard DCPDS data and resources. The controls were lacking because the DCPDS functional and acquisition program managers did not sufficiently recognize or define information assurance requirements, including the development of a comprehensive certification and accreditation plan. Separation of duties was also inadequate. Specifically, the acquisition program manager also had security certification and accreditation responsibilities. Without independent oversight, the acquisition program manager could define the DCPDS security safeguards, design them into the system, assess the adequacy of the safeguards, modify the safeguards, approve the safeguards, and accredit DCPDS for operations. As a result, DCPDS had high risks for unauthorized system access, intentional and unintentional alteration and destruction of data, and denial of service to authorized users.

Management had taken action in response to the report finding. The acquisition program manager assigned an information system security officer, and the Civilian Personnel Management Service developed an action plan to incorporate technical experts' recommendations on protection needs for DoD civilian personnel data and computer resources that process those data. A joint test team from the acquisition program management staff and the Air Force Information Warfare Center was to evaluate the technical suitability of encryption solutions. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) stated that a designated approving authority was appointed, and a facilitated assessment review process was conducted that included measures to mitigate risks when connecting to other systems. A certification and accreditation plan was in final coordination for signature.

Report No. 98-041, "Acquisition Management of the Defense Civilian Personnel Data System," December 16, 1997. The report concludes that the DCPDS functional proponent performed responsibilities normally expected of the acquisition program manager and the program executive officer. Therefore, the Air Force could not ensure that it was adequately managing the high levels of risk in essential areas of DCPDS testing, information assurance, and life-cycle costing. The report recommended that the Air Force revise the DCPDS acquisition management structure to clearly define the lines of

responsibility, authority, and accountability. It also recommended that the Air Force appoint a program executive officer to execute acquisition management and direction of DCPDS and appoint a program manager in accordance with DoD Manual 5200.52, "Acquisition Career Development Program," November 1995.

Actions taken by management satisfied the intent of the report. The Civilian Personnel Management Service and the Air Force more clearly defined the lines of responsibility, authority, and accountability for the acquisition of DCPDS, and the Office of Assistant Secretary of the Air Force (Acquisition) conducted a comprehensive in-process review of the program. The Air Force stated that it intended to appoint a Level III program manager.

Report No. 98-024, "Security Controls Over Systems Serving the DoD Personnel Security Program," November 19, 1997. The report states that the Defense Investigative Service did not have adequate controls to protect personnel security systems and data from compromise. Therefore, the Defense Investigative Service had insufficient assurance that it could prevent unauthorized individuals from accessing, modifying, or destroying the highly sensitive DoD personnel security information that the Defense Investigative Service administered. Without the guidance of a trusted facility manual to specify the required level of security, systems administrators implemented security controls that did not adequately protect critical portions of the network. The deficiencies would allow a user to access, modify, or destroy highly sensitive personnel information without leaving an audit trail. The security weaknesses would also permit a user to log onto the system without having a user account, to copy database files, to view sensitive system settings without authorization, and to potentially gain root access to the system. The Defense Investigative Service implemented its network using an open architecture, which left critical network components vulnerable to internal and external attacks. Because of physical security weaknesses, unauthorized personnel could have entered the center and obtained access to all Defense Investigative Service automated data, which included sensitive information, or could have stolen equipment. The report recommended that the Defense Investigative Service communicate specific security requirements, modify memorandums of agreement and contracts to include system security, develop and implement access control policies, isolate critical resources in the system architecture, and improve physical security.

The Defense Investigative Service concurred with the recommendations. Management prepared a trusted facility manual; updated its memorandums of agreement; implemented a security awareness program; implemented a segmented, isolated network architecture; installed devices and increased patrols to secure the Defense Investigative Service computer center; physically secured telephone cable rooms; and enforced the identification badge policy. Management stated that it had already implemented C2-like controls on critical portions of the Defense Investigative Service network and upgraded physical security.

Report No. 98-012, "Federal Acquisition Computer Network Central Contractor Registration (CCR) Program," October 22, 1997. The report concludes that the Central Contractor Registration database was subject to increased risk of improper access or disclosure of sensitive information. Additional security improvements were needed to ensure that the Central Contractor Registration System could accomplish the following:

- comply with Controlled Access Protection level C2 security requirements,
- protect the Central Contractor Registration System from unauthorized access, and
- protect Central Contractor Registration System data submitted over the Internet.

The report notes that the Defense Information Systems Agency had implemented digital certificates, which are password-protected, encrypted data files.

The Defense Information Systems Agency generally agreed with the findings and recommendations and stated that it upgraded the Central Contractor Registration System operating system to a C2-level security system on July 20, 1997. In addition, the Defense Information Systems Agency stated that it had two Central Contractor Registration System machines, referred to as CCR and CCRI. The two machines were not physically connected, and CCRI acted as a firewall for the CCR machine. The Defense Information Systems Agency stated that it used VeriSign encryption technology to provide positive identification of the site submitting the data, but that VeriSign did not encrypt the transmitted data.

Report No. 98-007, "General and Application Controls Over the Mechanization of Contract Administration Services System," October 9, 1997. The report concludes that the system had general and application control weaknesses. Control weaknesses over access to the Mechanization of Contract Administration Services system would allow unauthorized users access to sensitive data in the system.

The report recommended that Defense Finance and Accounting Service Columbus Center issue security guidance, periodically review users' levels of access, and terminate user accounts and privileges that were no longer necessary. The report also recommended that the Defense Logistics Agency Systems Design Center designate the employee and contractor application programming positions as critical-sensitive and require background investigations of personnel in those positions. System application software personnel with access to the critical-sensitive contract payment program code did not receive the required access designations and background investigations because of noncompliance with the appropriate DoD regulation. Defense Finance and Accounting Service management concurred and planned to issue security guidance to the personnel responsible for implementing employee-level security, periodically review the Mechanization of Contract Administration Services system to verify employee access to supervisory files and other sensitive files, and terminate user accounts and sensitive file access that were no longer required. Defense Logistics Agency management concurred with the

finding concerning background investigations and planned to direct the Commander, Defense Logistics Agency Systems Design Center, to prepare a plan to obtain background investigations of application programmers and appropriate contractor programmers. The Defense Logistics Agency Systems Design Center revised the sensitivity designations for a number of positions and conducted the necessary background investigations for personnel holding the positions. The Defense Logistics Agency Systems Design Center planned to review all remaining positions and perform the required background investigations. The Defense Logistics Agency Systems Design Center also planned to complete guidelines for position sensitivity designations for employees and contractors by December 31, 1998.

Report No. PO 97-049, "DoD Management of Information Assurance Efforts to Protect Automated Information Systems," September 25, 1997. The report concludes that the security safeguards and practices that protect DoD automated information systems that process sensitive-but-unclassified information from unauthorized access needed improvement. Inefficient and ineffective implementation of the DoD-wide Information Systems Security Program, outdated policies and procedures, inadequate direction and oversight, and lack of accountability for information systems security management controls contributed to the inadequate security safeguards.

The report recommended developing procedures to determine the Defense information infrastructure's security posture, developing an information assurance strategic plan, standardizing the automated information systems certification and accreditation process, centralizing the management of DoD-wide incident reporting and response, and incorporating accountability requirements for personnel responsible for safeguarding DoD automated information systems. The Acting Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) generally concurred with the finding and recommendations and, in coordination with the Services, Joint Staff, and Defense agencies, was establishing an integrated management process to extend DoD oversight of information assurance programs and activities to all DoD Components. Management developed the Defense-wide Information Assessment Program, which would facilitate establishment of a common baseline for the planning, coordination, assessment, integration, and oversight of DoD information assurance activities. Management also established a standard DoD security certification and accreditation process that includes standard security requirements to ensure uniform implementation of security safeguards for automated information systems DoD-wide. Further, management completed an assessment of DoD information assurance training and established an integrated-in-process team to implement the findings. The team was to recommend actions and policies to address such issues as identifying critical information assurance and information technology management knowledge and skills, creating a mechanism to assess and certify individuals, and developing training programs.

Report No. 97-216, "Security Over Networks Used to Transmit U.S. Special Operations Command Financial Data," September 18, 1997. The report states that the U.S. Special Operations Command had no assurance that its financial information, which processed and transmitted through several financial applications and networks, was secured against compromise. Assurance was

lacking because the U.S. Special Operations Command had not conducted the required risk analysis for its organizations to identify the threats and vulnerabilities to its network and had not established security measures related to accessing computer systems and financial applications. Therefore, the U.S. Special Operations Command financial data that supported the DoD consolidated financial statements for FY 1996 and following years may not have been reliable.

The report recommended that the Commander in Chief, U.S. Special Operations Command, conduct a risk analysis of the organizations' networks and of their entry points to other networks and obtain memorandums of agreement for safeguarding the financial systems with the designated approving authorities for networks to which the U.S. Special Operations Command was connected. Management concurred with the recommendations and planned to conduct risk assessments, by July 1998, of U.S. Special Operations Command unclassified systems that access financial data. Management also stated that, as risk assessments were conducted, it would determine a designated approving authority and initiate memorandums of agreement to specify security responsibilities. Responsive actions by management were ongoing.

Report No. 97-203, "Application Controls Over the Defense Joint Military Pay System Reserve Component," August 15, 1997. The report concludes that the application security environment structure and access controls were inadequate. As a result, knowledgeable users could manipulate application resources without detection, jeopardizing the integrity of Army and Air Force pay data. Inadequate security controls existed over individuals with sensitive access because positions were not properly designated critical-sensitive or required background investigations had not been completed and because of inadequate enforcement of security requirements.

The report recommended improvements in defining the security control structure for the Defense Joint Military Pay System (DJMS) and in controlling access to its sensitive resources. Defense Information Systems Agency management concurred with the recommendations and stated that Defense Megacenter Denver would provide written notification to information system security officers (ISSOs) of all security changes affecting DJMS, and the ISSOs would approve access to all Air Force DJMS resources. The report states that management completed those actions as of May 1, 1997. The Defense Megacenter Denver performed a review of sensitive Customer Information and Control System transactions and planned further reviews to evaluate necessary access levels by July 31, 1997. The Defense Finance and Accounting Service concurred with the recommendation to request access to all DJMS resources directly from the ISSOs and established procedures to request system access authorization through the DJMS coordinating ISSO. The Defense Finance and Accounting Service agreed that it had to aggressively emphasize the importance of security issues, and the Director, Defense Finance and Accounting Service, issued a memorandum requiring the Defense Finance and Accounting Service center directors to provide written assurance that they have complied with personnel security and suitability programs.

Report No. PO 97-024, "Management of Multilevel Security Applications for DoD Systems," June 12, 1997. The report identifies two conditions in need of management attention. DoD established requirements for multilevel security in automated information system acquisitions without fully identifying system operational and security requirements. DoD did not fully identify security requirements because DoD security policies and procedures for automated information systems were outdated and fragmented. DoD organizations were also developing and incorporating multilevel security technology into automated systems with limited coordination and oversight. The report states that the DoD multilevel security Program Office had not coordinated all DoD multilevel security initiatives because of inadequate authority and resources.

The report recommended that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) establish security policies and procedures unique to automated information systems, including the establishment of a standard certification and accreditation process, and develop a sensitivity labeling standard for automated information system data storage and processing with policy to implement it throughout DoD. The Assistant Secretary concurred and stated that a new security directive would be available in October 1997, and a March 1997 memorandum required the use of the DoD Security Certification and Accreditation process for information technology. In addition, the Assistant Secretary was coordinating a labeling policy.

A draft DoD regulation included a requirement for all DoD organizations to implement data labeling procedures. A March 30, 1997, memorandum from the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) requires the Defense Information Systems Agency and the National Security Agency to jointly lead the effort to ensure that all Unified commands and Service agencies adhere to the Secret-and-Below Interoperability process. A new DoD Multilevel Security Program Management Office was created with three personnel in addition to the four people and contractor support in place at the Defense Information Systems Agency. The Secret-and-Below Interoperability process mandates that the DoD Multilevel Security Program Management Office coordinate all secret-and-below requirements.

Report No. 96-214, "Computer Security for the Federal Acquisition Computer Network," August 22, 1996. The report concludes that the Defense Information Systems Agency (DISA) had not obtained capabilities for digital signatures or encryption for procurement transactions sent over the Federal Acquisition Computer Network (FACNET). As a result, FACNET transactions could have suffered undetected alterations, may not have satisfied legal requirements, and may have been subject to compromise. DISA had not established data backup procedures or developed the required continuity-of-operations plans for FACNET. As a result, the ability of FACNET to recover operations following a disaster was not assured. The DISA Electronic Commerce and Electronic Data Interchange Program Management Office (Program Management Office) had not provided adequate controlled access protection for FACNET. The Program Management Office did not implement security measures in FACNET to prevent unauthorized users from reading or modifying sensitive information. Specifically, the Program Management Office did not implement controlled access protection, which

includes identification and authentication, discretionary access control, auditing, and object reuse. Without controlled access protection, FACNET data were not protected from unauthorized users reading or modifying the data.

The report recommended that DISA develop a plan to implement digital signatures and data encryption, develop backup procedures, and enhance network security by implementing a firewall protection mechanism and by ensuring that FACNET complies with controlled access protection requirements. The Director, DISA, concurred with the recommendations in the draft report and stated that DISA had implemented or planned to implement corrective actions. DISA established the Electronic Data Interchange Security Working Group for the purpose of addressing electronic data interchange security policy and development of the security implementation plan consistent with DoD guidelines. In addition, DISA stated that it had developed standard backup procedures; established procedures to store backup data in a secure, off-site location; and planned to establish a backup facility at Slidell, Louisiana. The final report redirected the recommendations on limiting FACNET transactions and obtaining software encryption and digital signature capability to the Deputy Under Secretary of Defense (Acquisition Reform).

The Deputy Under Secretary of Defense (Acquisition Reform) limited FACNET transactions to the simplified acquisition threshold. DISA had established an ongoing analysis of the issues associated with obtaining a software encryption and digital signature capability for FACNET.

Report No. 96-179, "Followup Audit of Controls Over Operating System and Security Software on Computer Systems at Defense Megacenter, Mechanicsburg, Pennsylvania," June 27, 1996. The audit objective was to determine the adequacy of Defense Megacenter Mechanicsburg and Naval Inventory Control Point corrective actions, taken or planned, to improve general controls to respond to the recommendations made in Office of the Inspector General, DoD, Report No. 95-066, "Controls Over Application Software Supporting the Navy's Inventories Held For Sale (NET)," December 30, 1994. The report concludes that Defense Megacenter Mechanicsburg and the Naval Inventory Control Point had fully implemented 7 of the 11 previous recommendations. However, additional actions were necessary to improve general controls over the operating system and database management system.

The report recommended that Defense Megacenter Mechanicsburg improve controls over supervisor calls and restrict sensitive utilities in accordance with DISA guidance. The report recommended that DISA Western Hemisphere develop procedures requiring Defense megacenters to submit locally developed supervisor calls for an integrity review. Inadequate general controls made it possible for knowledgeable users to improperly access, modify, or destroy computer data and programs without detection. The Navy and DISA concurred with the recommendations, and planned corrective actions were fully responsive.

Report No. 96-175, "Computer Security Over the Defense Joint Military Pay System," June 25, 1996. The report states that controls were inadequate to limit application access to authorized employees and to limit authorized users

to the programs, functions, and data required to perform their duties. Definitions of responsibilities for authorizing and controlling access to DJMS were unclear, and users could improperly attain access to the payroll application. As a result, the integrity of the military pay data was vulnerable.

In response to the report recommendations, management took the following actions:

- frequently review the audit log for user access to the master pay datasets;
- change critical production datasets to read-only access to ensure proper separation of duties;
- remove the global-access-permission attribute from all sensitive profiles;
- conduct periodic reviews to ensure proper granting and control of access;
- create a Service-level agreement that includes the automated information system security requirements of DoD Directive 5200.28 and a clause allowing for future updates when needed;
- establish and designate the ISSO position at Defense Finance and Accounting Service Indianapolis as critical-sensitive;
- grant the ISSO at Defense Finance and Accounting Service Indianapolis the capability to view and monitor system access for users that have access to the DJMS;
- have the Director, Directorate of Military Pay, Defense Finance and Accounting Service Denver, assume responsibility for designating position sensitivity for all positions created within the directorate;
- verify that the sensitivity level assigned to all positions within the Directorate of Military Pay complies with DoD Regulation 5200.2-R; and
- inform all directors of procedures regarding sensitive positions.

Issues regarding a memorandum of agreement, which was to include the realignment of the directorate so that the ISSO reported directly to the Director, Directorate of Military Pay, were not resolved.

Report No. 96-172, "Certification and Management of Value-Added Networks," June 21, 1996. Value-added networks provide communication of electronic data between DoD and contractors. The audit objective was to determine the adequacy of the value-added network certification process and of the management and oversight of value-added networks. The report concludes that DISA did not perform reviews to verify that each value-added network maintained an audit trail of transactions, backed up all data to allow for full data recovery capabilities, and had an internal quality monitoring program to ensure the maintenance of reliable communication lines. Audit trails, data backup and recovery capabilities, and internal quality monitoring programs are measures that enable DoD and non-DoD organizations to verify when value-added networks are responsible for errors and omissions. DISA personnel stated that

they did not verify whether each value-added network had internal quality monitoring programs because of the lack of guidance on how to perform evaluations of those programs. The report states that until DISA added a remote testing feature, DISA could not be certain that DoD would be able to recover transaction information in the event of a disaster.

In response to the report recommendations, management took the following actions:

- establishing the capability to monitor all Government transactions being transmitted to value-added networks, which allows the Government to verify transaction processing and to retain an audit trail;
- annually recertifying the disaster recovery plans of the value-added networks;
- monitoring the supporting communications infrastructure; and
- expediting the completion and issuance of the revised Value-Added Network License Agreement.

Report No. 96-124, "Selected General Controls Over the Defense Business Management System," May 21, 1996. The audit objective included determining the adequacy of selected general and application controls for the Defense Business Management System. The report concludes that computer security at the Defense Finance and Accounting Service Financial Systems Activity Columbus, Ohio, did not adequately protect the Defense Business Management System development code from compromise and failed to ensure that only authorized program software changes were made. The Defense Megacenter and Defense Logistics Agency Systems Design Center, both in Columbus, Ohio, were inadequately prepared to react in the event of a disaster.

In response to the report recommendations, management reviewed, corrected, and validated user accesses; defined position sensitivity; published and implemented internal security policy; changed account deactivation for unused accounts from 180 days to 30 days; began providing security training through a variety of media and maintaining signed attendance records; established separation of duties between the systems management office and the program development staff; implemented formal code reviews for all program changes; performed a detailed disaster risk analysis and finalized the disaster recovery plan; placed the disaster recovery plans on hold pending the relocation of the computer lab to Defense Megacenter Columbus; and began performing backups of critical Defense Business Management System data files on a weekly basis.

Report No. 96-053, "Followup Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service," January 3, 1996. The report concludes that Defense Megacenter St. Louis, Missouri, adequately implemented all of the prior recommendations applicable to the systems that migrated to it. However, Defense Megacenter Denver, Colorado, needed to take additional corrective actions on 2 of 16 prior audit recommendations. Controls over sensitive features of the operating system needed further improvement. The report recommended that DISA Western Hemisphere

implement security controls to eliminate and prevent exposures related to supervisor calls. In response, management installed sensitive utilities so that parameters were properly defined and also implemented security software over the issuance of sensitive utility commands. Management replaced the supervisor call, redefined the parameters of a sensitive utility, implemented security software features so that only authorized users could issue commands for two sensitive utilities, amended guidance to restrict sensitive utilities to authorized security administrators, implemented a system for job security checking and auditing, and defined users by accessor identifiers according to user needs.

Report No. 95-264, "Defense Finance and Accounting Service Work on the Air Force FY 1994 Finance Statements," June 29, 1995. The report concludes that Defense Finance and Accounting Service (DFAS) Denver did not adequately monitor security over the Merged Accountability and Fund Reporting (MAFR) System. Lack of adequate monitoring occurred because DFAS Denver did not designate a security manager for the MAFR System, did not perform periodic reviews to determine whether individuals had a continued need for access, and lacked written procedures for system security oversight. Individuals could retain access that they no longer needed, thus retaining the ability to update, change, or modify MAFR System files. Proper monitoring would reduce the risk of unauthorized access and system use and loss of accountability and control over Government data. The MAFR System did not maintain audit trails or transaction histories for transactions originating at DFAS Denver because at the installation of the system, DFAS Denver did not consider audit trails for DFAS Denver adjustments to be necessary. As a result, we could not determine which transactions were initiated by DFAS Denver personnel who had MAFR System access; whether the adjustments had adequate support; and whether they were properly classified, coded, and recorded in each affected account. The MAFR System had been designated an interim migratory system. DFAS Denver was including modifications to the MAFR System in the Defense Cash Management System. The new system would include the necessary audit trails for transactions originating at DFAS Denver. Because management had corrective actions in progress at the end of the audit, the report contained no recommendations.

Report No. 95-263, "Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service," June 29, 1995. The audit objective was to determine the adequacy of corrective actions by DISA Western Hemisphere and the Defense Logistics Agency Systems Design Center to improve computer security. The report states that although significant improvements had been made, 20 of 87 prior recommendations required additional corrective action.

The report recommended improvements in operating system and security software, environmental controls, and management controls. In response to the recommendations, management initiated actions to review all unauthorized program facility libraries and programs and to delete obsolete and undocumented programs; to review the access rules of all authorized program facility libraries and to protect libraries as required; to develop controls within the service calls to eliminate identified integrity exposures; to review bypass

label processing and to allow access only to tape files; to install overhead shutoff valves; to identify sensitive utilities that were not in the protected program list, place them in the protected program list, and monitor their use; to conduct certification testing; and to publish the DISA Western Hemisphere Security Handbook.

Report No. 95-259, "Internal Controls for the Military Sealift Command Portion of the Transportation Business Area of the FY 1994 Defense Business Operations Fund Financial Statements," June 28, 1995. The report states that general controls for accessing and accountability over the Unit-Level Billing System were ineffective, making the systems and data vulnerable to unauthorized access and alteration. The computer security personnel did not have adequate training or supervision, and they did not follow policies and procedures regarding access to the system or accountability of user identification codes.

Management concurred with all the recommendations and planned to implement actions or policies to verify user need and level of access, delete a user's programs and files after removal of the user identification codes, cancel user identifications after termination of employment, define access levels, develop logon accesses that do not degrade system performance, track unauthorized access attempts, provide training in access control software, and properly supervise computer security staff. Management either had completed planned actions or was in the process of completing them.

Army Audit Agency

Report No. AA 99-5, "Information Systems Security Program Phase II Follow-On Validation," October 15, 1998. This report is a follow-on to Report No. AA 97-214, "Information Systems Security Program," June 30, 1997. The audit evaluated the adequacy of operational and electronic aspects of the Army's Information Systems Security Program and assessed the extent to which sensitive but unclassified sustaining base networks and information systems were vulnerable to attack. The report states that although the Army had made improvements, its sensitive but unclassified information systems may still have been vulnerable to attack. The vulnerabilities existed because of a general lack of emphasis, guidance, and assigned responsibility for information systems security; outdated policies and procedures; ineffective practices and procedures used in the certification and accreditation process; information systems security plans that were either non-existent or that did not address key computer security components; security hardware and software that had not been effectively deployed; training programs that did not reach all personnel or provide the necessary technical training; and the lack of a process for identifying information systems security funding requirements. The report recommended mapping key elements of the networked information system, revising the certification and accreditation process, and limiting networked computer features and services to those required for operations. Management implemented mapping of key elements and agreed to revise the certification and accreditation process and limit access to applications and services. The

estimated completion date was January 1, 2000. The report also recommended developing risk assessments, including information systems security in strategic plans, and requiring that those documents be provided to the Office of the Director of Information Systems for use in the Army annual assessment plan. Management concurred with the recommendations and took or planned actions to implement the recommendations. Additionally, the report recommended adding new metrics and rewording existing metrics to address identified security weaknesses. Management agreed and estimated completion by April 1, 1999. Further, the report recommended that the Army complete and implement an annual assessment plan. Management concurred and estimated a completion date of August 31, 1999.

Report No. AA 98-265, "Security of Total Asset Visibility," June 30, 1998. The Total Asset Visibility capability is a fully automated, near real-time logistics management tool designed to provide complete integrated visibility of Army assets and other logistical data. The purpose of the capability was to improve materiel readiness and inventory management and to lower costs. The capability provides information essential to making materiel management decisions. The capability provides users throughout the Army logistics community with the ability to track assets in use, in storage, or in transit. The capability also provides information on requirements, authorizations, force structure, weapon systems configurations, and catalog data. The report concludes that the procedures for monitoring user access were not always effective. For example, security officers did not review access control records to make sure only authorized personnel had access, and management did not terminate access for some users who had not used the system within 30 days for new users and 6 months for prior users.

The report recommended that management complete the following:

- provide security officers, annually, a list of authorized Total Asset Visibility users and require the security officers to certify that the users are still authorized access to the system; terminate access for users who are no longer authorized; and temporarily suspend access to users whose authorizations are in doubt and
- review user activity at least every 6 months and terminate access for new users who have not used the system within 30 days of receiving access, or prior users who have not used the systems in the past 6 months.

Management nonconcurred with the recommendation that the security officer be responsible for terminating a nonauthorized account. Management responded that unless the security officer received notification to terminate an account, that account was kept active, and no practical or cost-effective method existed for identification and termination. Management added that because the problem was systemic throughout DoD computer systems, it required high-level attention and resources. However, the report reiterated that the Army must take the remedial action recommended. Management concurred with the recommendation that it would terminate accounts that were not used within 30 days of granting access or that had not been used in 6 months.

Report No. AA 98-170, "Unit-Level Logistics System-Ground," April 29, 1998. The Logistics System automates supply and maintenance operations and the process for reporting equipment readiness and use at the unit level throughout the Army. The report states that the Army did not effectively use the System to manage supply and maintenance operations, keep accurate data in system files or use system reports for managing operations, collect accurate data on equipment readiness, provide effective automation training, and maintain proper security.

The report recommended that system management security do the following:

- include the Logistics System in information system security programs and provide oversight for such systems;
- provide milestone schedules for implementing recommendations to monitor progress and ensure completion;
- review all computers on which the Logistics System operates to verify that only DoD-approved virus protection software is installed, passwords are properly assigned and controlled, and generic passwords are deleted or changed;
- prepare security standing operating procedures that include all security countermeasures necessary to adequately safeguard the Logistics System and distribute the security procedures after approvals have been obtained;
- test DoD-approved virus protection software whenever significant changes are made to either the system or virus protection software and provide users with special instructions for installing DoD approved virus protection; and
- include instructions for deleting or changing the generic password when fielding software changes.

Management generally agreed with the recommendations and said that it had taken or would take corrective actions.

Report No. AA 98-123, "Information Assurance for the Army's Segment of the Defense Civilian Personnel Data System," March 3, 1998. The audit objective was to determine whether implementation of the Army Information Systems Security Program within the Army interim Civilian Personnel Regionalization System and the Army segment of the Defense Civilian Personnel Data System effectively protected Privacy Act data from unauthorized access. The report concludes that civilian personnel data were not effectively protected from unauthorized access because the Army did not effectively implement its Information Systems Security Program. Specifically, management did not do the following:

- appoint a system-level information systems security manager to manage and oversee information systems security,
- require system accreditation,
- require a system-level risk assessment,

- require the development and distribution of information systems security training information,
- configure security software or turn on and monitor audit logs,
- perform the necessary security assessments, and
- develop a comprehensive certification and accreditation plan.

As a result, Army civilian personnel systems and Privacy Act data were highly vulnerable to unauthorized access, malicious attack, exploitation, compromise, and denial of service. In addition, unauthorized personnel could use security weaknesses in the interim civilian personnel systems of the Army to gain unauthorized access to other systems because of trusted relationships between Army civilian personnel systems and other systems within and outside DoD.

The Office of the Deputy Assistant Secretary of the Army (Civilian Personnel Policy) said that it would establish a system-level program, establish and appoint a system-level security manager, and conduct a system-level risk assessment.

The Office agreed to do the following within 6 months of completion of the system-level risk assessment:

- implement appropriate safeguards and countermeasures to protect Privacy Act data;
- develop and distribute information systems security plans, policies, procedures, and manuals for the interim system; and
- identify and initiate appropriate security training for systems administrators and users of the system.

Management expected to implement its planned actions by December 31, 1998.

Report No. AA 98-10, "Army Web Server Security," January 20, 1998 (FOUO). The report states that Army policies and procedures did not adequately identify safeguards associated with the security of web servers and the Internet. Also, it states that manager training and user awareness programs did not adequately address those issues.

The Director, Information Systems for Command, Control, Communications, and Computers, concurred with the recommendations and planned the following actions:

- expand, revise, and develop information security publications to include policy on web security and related issues, with final publication by the fourth quarter of FY 1999;
- incorporate recommended changes in the on-line registration process and require Army organizations to certify the security of their web servers as part of the revised homepage registration process;
- establish web manager training in the Army System Administrators Course at the Computer Science; and

- develop an Internet users' guide that would be incorporated into the Army Homepage, and possibly incorporate the guide in future updates of information security publications.

As of October 1, 1997, management established procedures to incorporate recommended changes in the on-line registration process and to certify the security of the web servers. As of December 1, 1998, management planned to issue revised information security publications by September 30, 2000; establish web manager training by September 30, 1999; and develop an Internet user's guide by September 30, 1999. As of December 1, 1998, the Army had completed some of the recommendations and was continuing action on the remaining recommendations.

Report No. AA 98-32, "Army Working Capital Fund FY 97 Financial Statements, Crane Army Ammunition Activity, Crane, Indiana," November 17, 1997. The report states that personnel at the Defense Accounting Office - Red River Army Depot, and later transferred to DFAS Operating Location Rock Island, did not adequately protect passwords for access to the Standard Industrial Fund System and the Standard Financial System Redesign-1. Inadequate password protection occurred because formal password management procedures were not in place at the Defense Accounting Office. The report recommended that DFAS Indianapolis make sure that procedures are in place at Operating Location Rock Island to delete passwords when necessary, make supervisors responsible for the system access of their employees, request that information system managers set up password change procedures, and require supervisors to give initial and periodic security training to employees. DFAS Indianapolis concurred with the recommendations and stated that system administrators periodically reviewed access to automated systems, supervisors were responsible for requesting user access and deletions, and systems automatically required password changes. As of December 1, 1998, the Army had taken action on some of the recommendations and continued action on the remaining recommendations.

Report No. AA 98-28, "Audit of Controls Over Computer Resources, U.S. Army Training Center and Fort Jackson, Fort Jackson, South Carolina," November 17, 1997. The report identifies weaknesses with accounting for and securing computer hardware and software. The report also states that access controls for the Installation Support Module and the Army Management Information System were generally adequate but had weaknesses in the area of password management. The Information System Security Officer did not make annual reviews to retire the passwords of users who were separated from the duties or functions for which the passwords were assigned. Because of the password management weakness, unauthorized personnel had an increased opportunity to access the computer systems. The report was not subject to the official command-reply process, so it did not include formal comments. The report suggested that management accomplish the following to account for and secure computer hardware and software:

- conduct a complete inventory of items in storage,
- establish security measures to protect computer resources kept in storage areas,

- reemphasize the need to properly account for computer hardware acquisition,
- establish procedures and a standardized training program for managing copyrighted software, and
- conduct annual inspections to ensure that only authorized and supported software is on computer systems.

Management agreed with the recommendations and planned to have all corrective actions completed by June 30, 1998. The report also suggested that the Information System Security Officer annually review the systems to identify and remove old and dormant passwords. Management concurred with the suggestion and planned to hire an information security manager who would be responsible for conducting an annual review to identify old and dormant passwords.

Report No. AA 98-9, "Web Server Security, U.S. Army Aviation and Missile Command, Redstone Arsenal, Alabama," October 31, 1997 (FOUO). The report states that Privacy Act information for about 224,000 civilians was accessible to the public over the Internet when personnel at Redstone Arsenal, Alabama, placed data from the Army Civilian Personnel System in an unprotected subdirectory on a web server. A contract employee at the Training Application Branch, Corporate Information Center, Army Aviation and Missile Command, used the data to develop an Internet capability to extract demographic data about personnel taking training courses. The command's webmaster and web-site security manager were not aware that the data were available to users visiting the organization's web site because the web page contained no hyperlinks or gateway interface scripts that would lead visitors to the data.

The Army Aviation and Missile Command generally concurred with the recommendations and stated that it had placed a developmental server behind a firewall on July 1, 1997; issued a command-wide message on September 15, 1997, requiring all Internet webmasters to conduct complete inventories of information on their web sites; and agreed to begin routine Internet security briefings and training in October 1997. The Army Aviation and Missile Command noted that the Defense Information Systems Agency Global Operations and Security Center had completed a vulnerability analysis in March 1997, and 95 percent of the identified vulnerabilities were corrected by September 1, 1997. The Army completed actions on the recommendations.

Report No. AA 98-2, "Unit-Level Logistics System-Ground, XVIII Airborne Corps and Fort Bragg, Fort Bragg, North Carolina," October 9, 1997. The report states that units of the XVIII Airborne Corps and Fort Bragg did not use the most effective antivirus software and did not adequately control system passwords. As a result, systems were vulnerable to attack by viruses and unauthorized individuals. Those conditions existed because Information System Security Officers did not adequately monitor antivirus software and because commanders and supervisors did not monitor and enforce password controls.

The command concurred with the recommendations and stated that the Corps Information Systems Security Management Office issued a memorandum

emphasizing the policy on antivirus software and password controls, a directive covering antivirus software policy, and a memorandum reminding Information System Security Officers to include Logistics System computers in periodic inspections. Management implemented the recommendations as of December 4, 1997.

Report No. AA 97-306, "Unit-Level Logistics System-Ground, 3d Infantry Division (Mechanized) and Fort Stewart, Fort Stewart, Georgia," September 26, 1997. The report states that units using the system did not have current antivirus software operating on their computers, and access controls were not adequate. Those conditions occurred because the Logistics System computers were not under the installation's automated information system security program. The report recommended that management include the Logistics System in the automated information system security program and that units have adequate password controls. Management concurred and issued a memorandum in January 1997 to establish procedures for updating antivirus software, ensuring adequate password protection, and including Logistics System computers in future automation security inspections.

Report No. AA 97-293, "Army Working Capital Fund FY 97 Financial Statements, Rock Island Arsenal, Rock Island, Illinois," September 26, 1997. The report states that access controls over the Standard Industrial Fund System needed improvement. Both Rock Island Arsenal and Anniston Army Depot held responsibilities for controlling access to the Standard Industrial Fund System. The report states that controls were adequate to prevent access without a valid password and user identification, but controls were not adequate to prevent authorized users from accessing data that they did not have a need or the authority for. That condition existed because users received general levels of access rather than receiving access tailored to each user. The report notes that the command was in the process of improving controls for changing passwords, so a recommendation for additional controls was not necessary.

The report recommended that management change the levels of access so that users have access only to the information and capabilities necessary to do their jobs. Management agreed that it should examine access levels but stated that tailoring levels of access for each user would significantly increase workload and would become unmanageable. Management proposed assigning sensitive capabilities to a separate access level and allowing only selected users access to that level. The report states that the proposed actions would meet the intent of the recommendation by greatly reducing the number of personnel with the capability to change the general ledger without leaving an audit trail. Management implemented the planned actions as of November 7, 1997.

Report No. AA 97-767, "Performance Measures for Information Systems Security," August 15, 1997. The report presents the results of the process used to develop installation-level performance measures for assessing the effectiveness of information systems throughout the Army. Along with the Defense Information Systems Agency Operational Process Improvement Office, the Army Audit Agency sponsored an information security strategic planning workshop in April 1997 and an information systems security performance measure development workshop in June 1997. The workshops were a result of Army Audit Agency Report No. AA 97-214, "Information Systems Security

Program," June 30, 1997, which states that the core processes that the Department of the Army and Army installations used to manage and implement the Army Information Systems Security Program required reengineering.

As a result of the workshops, the Command and Control Project Triad approved seven performance measures on June 18, 1997. The following performance measures were to be used to hold commanders accountable for their information systems security program outcomes:

- the percentage of available time that required intrusion protection, detection, and monitoring devices are operational;
- the availability ratio (actual on-line time compared with total required on-line time);
- the percentage of users with user profiles;
- the percentage of budget allocated to information assurance;
- the percentage of allocated dollars obligated on information assurance;
- the percentage of system administrators and network security managers that received and completed formal system administrator training; and
- compliance with the National Security Telecommunications Information Systems Security Document 600 and Army Regulation 380-53.

The report contained no recommendations.

Report No. AA 97-214, "Information Systems Security Program," June 30, 1997 (FOUO). The audit objective was to determine the extent to which unclassified-sensitive sustaining base networks and information systems at Army posts, camps, and stations were vulnerable to attack. The report concludes that the unclassified-sensitive sustaining base networks and information systems of the Army were highly vulnerable to malicious attack; exploitation; compromise; denial of service; and, in the most extreme cases, destruction by computer hackers. The vulnerabilities existed because either automated security controls were not adequate or management did not adequately use controls to prevent and detect unauthorized intrusion and access to sustaining base information.

The Office of the Director of Information Systems for Command, Control, Communications, and Computers concurred with the recommendations and drafted a policy memorandum to emphasize information systems security and to establish responsibilities and training. The Secretary of the Army and the Chief of Staff, Army, signed the policy memorandum on June 19, 1997. The Office of the Director also stated that, in response to the recommendation to reengineer the Army Information Systems Security Program, it had integrated corrective actions and timelines into the Information Operations Campaign Plan. The target date for completing planned actions was the first quarter of FY 1999. The planned actions were completed as of June 19, 1997.

Report No. AA 97-53, "Combat Service Support Control System," December 12, 1996. The report states that security requirements for the Combat Service Support Control System (the Control System) were generally satisfied when the system was tested in June 1994, but management could update security further to reduce vulnerabilities. Those vulnerabilities included unauthorized intrusion and access. The report also states that the Control System accreditation plan adequately defined security risks but needed to improve system countermeasures.

Management concurred with the recommendations and agreed to complete the security enhancement plan by June 30, 1997. Management consulted with the Defense Information Systems Agency and the Director of Information Systems for Command, Control, Communications, and Computers to obtain software security packages. Management also agreed to coordinate with DISA to identify opportunities to retest the Control System against intrusion. Management stated that the designated approving authority would finalize the accreditation plan in early 1997. As of December 1, 1998, the Army had implemented the planned actions.

Report No. AA 96-28, "Audit of U.S. Army Corps of Engineers Financial Management System (CEFMS) - Phase I," November 8, 1995. The report states that the Army Corps of Engineers Financial Management System (the Financial Management System) access control table effectively limited and controlled access to financial information, but users had the ability to circumvent the table by using structured query language. The Corps of Engineers did not design the Financial Management System to restrict access to sensitive Privacy Act data when users entered the system through other applications (such as structured query language) on the mainframe.

The report recommended that the Corps of Engineers review system tables, identify all sensitive data subject to the Privacy Act, and remove public access from those tables; issue guidance to database administrators on managing and restricting access to sensitive data; train employees in the proper use of sensitive information; and program the Financial Management System to provide a warning of user responsibilities to protect sensitive data. The report states that the Corps of Engineers had taken corrective actions to restrict access to sensitive data, including implementing security measures to remove public access from certain tables and to exclude sensitive fields from database views. The report states that the actions were adequate but that the Corps of Engineers should also restrict access to other personnel identifying data such as employees' home addresses and telephone numbers.

Report No. NR 95-428, "Financial Reporting of Wholesale Assets," June 19, 1995. The report states that commodity commands used several different programs to enter inventory transactions into the Commodity Command Standard System. Other individuals and organizations also used the programs, but access controls were not in place to prevent unauthorized users from creating inventory adjustments or requisitions. Also, the system did not provide an adequate audit trail to identify those who made an inventory transaction. That condition existed because access control procedures were not specific enough.

The report recommended that management implement controls to restrict the ability to make inventory adjustments to authorized personnel only, control and manage passwords based on user need, reduce the number of data entry programs used to enter critical transactions, and identify other transaction types that may require limited access. Management concurred and stated that it sent a memorandum to its subordinate commands asking for an evaluation of feasibility and costs. The planned date for an implementation plan was the end of FY 1995. As of December 1, 1998, the Army had implemented the planned actions.

Report No. SR 95-722, "Controls Over Reserve Component Pay," April 21, 1995. The report concludes that the controls over the Army Reserve pay system worked as intended but needed improvements. Most units had weaknesses over access controls to the automated drill attendance reporting software and an absence of appropriate separation of duties. Units did not change user passwords regularly or deactivate them after a user no longer required access. Commanders tasked personnel with access to the reporting software, generally the unit pay administrators, with additional responsibilities. Assigning the responsibilities to one person compromised key management controls and could have allowed intentional overpayments to go undetected.

The report recommended that the command program a control into the reporting software that requires users to revalidate logon identifications and change passwords every 90 days or it locks the user out of the software. It also recommended that the command direct units to separate responsibilities. The Army Reserve Command agreed and was implementing the recommendations. Therefore, the report did not include those issues as a finding and did not require a command reply.

Naval Audit Service

Report No. 059-95, "Selected General Controls at Defense Megacenter Mechanicsburg, PA," September 26, 1995. The report concludes that selected general controls at Defense Megacenter Mechanicsburg were not operating effectively and efficiently. Classified tape cartridges and round tapes were stored improperly, and entry access controls were improperly maintained. The Defense Information Systems Agency (DISA) had not issued official guidance on an automatic data processing physical security program. Defense Megacenter Mechanicsburg did not have a functioning internal management control program and did not properly designate critical-sensitive, noncritical-sensitive, and nonsensitive automatic data processing personnel. Management did not understand and did not follow DISA guidance for designating automatic data processing personnel. By not establishing an internal management control program as required by DoD Directive 5010.38, Defense Megacenter Mechanicsburg lacked controls to safeguard funds, property, and other assets against waste, loss, unauthorized use, or misappropriation. Unauthorized access could result in the deliberate destruction or theft of computer hardware, system software, customer application programs, or data files. Additionally, Defense Megacenter Mechanicsburg lacked operating

procedures to document and approve system software changes. Insufficient control of changes to system software presents the opportunity for manipulation of the system and could cause disruption or loss of data.

Management agreed with the findings and recommendations and submitted a waiver to permit "open storage" of classified cartridges and tapes; issued draft guidance to address physical security issues; conducted periodic reviews of access listings and removed access because of inactivity or changes in access privileges; reviewed access-level assignments; and developed, issued, and implemented change management procedures. Management also contracted to install a card-key access system at Defense Megacenter Mechanicsburg, included procedures for maintenance and reconciliation of access listings and the access card-key system in the DISA Western Hemisphere security handbook, and completed actions to change personnel designations to critical-sensitive where necessary.

Air Force Audit Agency

Project No. 98054006, "Equipment Inventory, Multiple Status, Utilization Reporting Subsystem Financial Controls," September 9, 1998. The Reliability and Maintainability Information System contains the only complete Air Force aerospace vehicle inventory and provides essential financial information. The audit determined that the lack of accreditation, contingency planning, and inventory documentation impaired system security. System accreditation lacked management attention because it was not separately funded. The report states that because of a lack of written instructions to support access controls and inadequate access procedures, operational personnel did not have assurance that the system adequately safeguarded data and prevented data alteration. Also, the application controls did not provide adequate audit trails, transaction histories, or file data verifications. Management agreed with the conclusions and recommendations and took or planned responsive actions. During the audit, management issued an operating instruction to approve, monitor, and periodically validate system-level access and user accounts. To improve the general controls, management agreed to appoint an appropriate designated approving authority in accordance with the applicable guidance and provide a certification completion plan by December 31, 1998. Management stated that it would request that the designated approving authority provide resources to achieve accreditation. The estimated completion date was March 31, 1999. Further, management was to develop and resource a contingency plan by December 31, 1998. Management was to have recorded all Reliability and Maintainability Information System computer equipment in the appropriate inventory by October 30, 1998. To improve the application controls, management agreed to restrict access to the unit cost field by December 31, 1998. Management was to include audit trails and transaction histories in the requirements for the replacement system. Estimated completion was March 31, 1999.

Project No. 98066011, "Application Controls Within the Defense Material Utilization and Disposition Program Management System," August 4, 1998. The Defense Material Utilization and Disposition Program Management System (the System) is a financial management system that identifies excess inventory and assets available for withdrawal from the Defense Reutilization Management Office. The report states that the System did not meet General Accounting Office application control standards for transaction authorization, system access, transaction histories, audit trails, error correction, and system reviews. The Air Force Materiel Command concurred with recommendations to strengthen the internal controls and to ensure that the system complies with laws and regulations. Management required the system manager to improve transaction controls by developing an automated approval process and required self-inspection reviews of signature approval compliance until the implementation of an automated approval process. Management planned to request that DISA establish access controls that restrict user access to specifically authorized systems. The Air Force Materiel Command also planned to issue guidance that would implement transaction histories and audit trails and establish procedures for correcting errors. Further, management planned to perform the required system review.

Project No. 97066028, "Information Protection Metrics and Measures Program," June 22, 1998. The Air Force established a metrics and measures program to track compliance with and the effectiveness of the Air Force computer information protection policy (the Policy). The Air Force implemented the Policy to ensure confidentiality, integrity, and availability of Air Force data. The report states that the Air Force could improve the adequacy of information protection program metrics and measures. The Air Force could more effectively monitor the progress of system accreditation if major commands identified systems as high-risk network systems or low-risk stand-alone systems. For example, a major command retained data that showed that they accredited 99 percent of their high-risk network systems. The Air Force could assess the effectiveness of the system accreditation process if major commands reported whether intrusions were to accredited or nonaccredited systems. The report notes that the Air Force could better determine the cost benefit of implementing additional safeguards if major commands reported the damage and recovery costs of intrusions. The report also states that the major commands did not accurately or completely report metrics data for information systems accredited, security awareness training, and education training. Those conditions occurred because major command officials did not establish procedures to effectively accumulate and report metrics data, and base-level officials placed insufficient emphasis on the data collection effort. Major command officials were not aware of requirements to maintain supporting documentation. As a result, the Air Force did not have essential information for allocating resources to correct potential security policy issues. Management concurred with the recommendations and planned to develop new metrics and establish procedures for major commands and bases to accumulate complete and accurate metrics. Management planned to incorporate the new metrics and procedures in a revised Air Force instruction.

Project No. 97066030, "Information Assurance for the Defense Civilian Personnel Data System at Air Force Locations," June 22, 1998. The Defense Civilian Personnel Data System (DCPDS) was to provide automated personnel support for civilian employees. The report states that for DCPDS, the Air Force must provide information assurance for personnel data covered by the Privacy Act. The report states that the Air Force did not perform a risk analysis and system certification, did not implement system security features such as audit logs and lockout protection, and did not encrypt sensitive but unclassified personnel data that would be transmitted over the Internet. As a result, the Air Force cannot detect or prevent unauthorized access, manipulation, or destruction of sensitive personnel data. Management agreed with the recommendations and had taken or planned responsive actions.

Project No. 97066033, "Information Protection - Implementing Controls Over Known Vulnerabilities in Air Combat Command Computers," May 19, 1998. The audit objective was to determine whether network managers implemented countermeasures to known vulnerabilities in networked computers at Air Combat Command locations. The report states that the Air Combat Command network managers for 15 of 40 network computers did not implement effective countermeasures to four vulnerabilities previously identified by the Air Force Computer Emergency Response Team from November 1996 through February 1997. As a result, approximately 18,000 Air Force computers and associated data were vulnerable to attack and subsequent compromise or destruction of stored information. The report contained no recommendations because management officials initiated the appropriate actions.

Project No. 97068016, "Application Controls Over Unit Price Data Within the Requirements Data Bank System, Air Force Working Capital Fund," January 27, 1998. The report states that the Requirements Data Bank integrates Air Force processes that compute procurement and repair requirements for spares, repair parts, and major equipment items. The main audit objective was to determine whether application controls over unit price data within the Requirements Data Bank were adequate for the system to produce accurate, complete, and reliable information. The report concludes that access controls to subsystem data and programs were inadequate. Several individuals had access to the system even though they had retired or left Air Force employment. Additionally, the subsystem did not retain 2-year transaction histories for unit price changes. The system manager and the Requirements Data Bank program offices were not aware of the Air Force requirement for retaining transaction history data and files for at least 2 years.

The report contains no recommendations because management initiated corrective actions during the audit. The system manager agreed to maintain a record of all users with system access and to periodically validate the record with DISA access listings and user supervisors. The program office removed system access for the individuals no longer employed by the Air Force. The Air Force Materiel Command security officer agreed to issue guidance clarifying access controls to all command functional system managers.

Project No. 97066029, "Global Combat Support System-Air Force," November 19, 1997. One audit objective was to determine whether Global Combat Support System-Air Force (the Support System) management addressed system security. The purpose of the Support System program was to incrementally modernize, integrate, and migrate standard software applications to operate in an open systems environment with a single, logical, integrated database. The Standard Base-Level Supply System was the first of 18 systems scheduled for modernization under the Support System contract. The report concludes that management did not identify specific security requirements or procedures to prevent data aggregation, obtain a risk analysis from Standard Base-Level Supply System officials, and identify a designated approving authority. Without designated approving authority involvement, the Air Force could approve unaccredited systems for operational use.

Responsive actions initiated by management include drafting the "GCSS-AF [Global Combat Support System-Air Force] Security Policy," which accomplishes the following:

- describes how the automated information systems must track their specific system security requirements,
- details the importance of the initial risk analysis, and
- states that the support system program office would list the designated approving authority for each automated information system in the implementation plan.

Management also initiated a three-step plan to resolve data aggregation problems. The plan consists of determining sensitivity levels of aggregated automated information systems, developing a guide that determines the classification of aggregated data in the shared data environment, and presenting the findings to the prime contractor for inclusion in system development.

Project No. 97066024, "Followup Audit -- Risk Management of Depot Maintenance Computers," November 7, 1997. The report presents an evaluation of management actions taken in response to Air Force Audit Agency Project No. 94066006, "Risk Management of Depot Maintenance Computer Systems," April 17, 1995. The followup report states that the management actions in progress would correct all but one condition mentioned in the original report. The Air Force had not yet updated its policies to require system developers to certify that new hardware and software met minimum security requirements. As a result, managers could not identify, assess, and manage computer security risks.

The report recommended that the Air Force provide guidance requiring proper certifications. The Air Force concurred and stated that developers were already required to certify and accredit software delivered on a hardware platform. The Air Force also stated that it would issue an instruction to clarify guidance on certification procedures.

Project No. 96068016, "Controls Over Stock Control and Distribution System Data Modification," August 21, 1997. The audit objective was to determine whether management had adequate controls over using the CA-Dataquery capability to access and change data in the Air Force Materiel Command (AFMC) Stock Control and Distribution system. The report concludes that AFMC Director of Logistics personnel did not adequately control CA-Dataquery use in the Stock Control and Distribution system. Personnel and application programmers from the software maintenance contractor with CA-Dataquery access made more than 2.4 million untraceable changes to the Stock Control and Distribution system. The AFMC Director of Logistics did not realize that, for changing production data, CA-Dataquery had controls weaker than the established transaction processing procedures. CA-Dataquery bypassed all system input controls and did not create acceptable transaction histories or audit trails.

The report recommended that the AFMC Director of Logistics remove the CA-Dataquery data modification capability from the Stock Control and Distribution system production region and process changes using established transaction processing procedures. Management concurred and stated that in the long-term, it would reengineer the system under the Global Combat Support System concept. In the interim, management said that it will increase controls over using CA-Dataquery to change data in the system's production region.

Management noted that because of system interface problems, it might need to use CA-Dataquery in the interim as an emergency solution to prevent work stoppages. For the event that selected personnel would need to make emergency corrections in the new system, management planned to develop a new "records adjustment" transaction that would be visible on accountable transaction records and that would identify the source of the corrective action. The Air Force Audit Agency concurred with management comments and alternative actions planned and said that it would evaluate the effectiveness of the new procedures in later audits.

Project No. 96066029, "Application Controls Within the Comprehensive Engine Management System," July 11, 1997. The report states that the Comprehensive Engine Management System did not retain complete transaction histories for 2 years, generate an adequate audit trail, or prevent unauthorized access to data and programs. The report states that those conditions occurred because the system program office and system designers were unaware of the requirements for retaining transaction histories and for having complete audit trails. As a result, users could not validate that data were available to support all transactions for more than 6,900 engines, valued at more than $8.5 billion, and a risk existed that an unauthorized person could destroy system data.

The report recommended that the Product Group Manager for Propulsion (Air Breathing) (SA-ALC/LR) require the Comprehensive Engine Management System program office to modify the system to include a user identification for changes to system tables. Management concurred and programmed the system in January 1997 to identify the user who makes a change to a table, creating an audit trail. The report also recommended that the AFMC Director of Financial Management and Comptroller distribute guidance to ensure that personnel are aware of General Accounting Office requirements for retaining transaction

histories and having complete audit trails. AFMC concurred and distributed a memorandum, dated May 30, 1997, to all Command organizations detailing the General Accounting Office requirements. To correct access control deficiencies, the report recommended that the Air Force require the Comprehensive Engine Management System to restrict the access granted to database administrators and application programmers by removing users' capabilities to update the production source code; restricting database administrators' capabilities to control all "update," "compile," and "move" functions of program changes; and removing system security administrative capabilities from all users and limiting those capabilities to DISA. The Product Group Manager for Propulsion (Air Breathing) (SA-ALC/LR) concurred and made system changes to implement the recommendations in March 1997. The report also recommended that AFMC notify system managers and users of the importance of proper access and separation-of-duty controls. AFMC concurred and stated that the letter of May 30, 1997, included access and separation-of-duty standards. Management completed all corrective actions before the final report was issued, so no followup action was necessary.

Project No. 97054014, "General and Application Controls Within the Consolidated Analysis and Reporting System," June 2, 1997. The report states that access controls over the Consolidated Analysis and Reporting System needed strengthening because the system programmer had access to both the program library and current data files. That condition could allow a single individual to make changes to records without proper authorization, audit trails, or identification. The report also states that more than 18 percent of sampled off-base users no longer required access to the system. In addition, the report states that users had access to a query language utility program that could allow them to change programs and data without passing normal system edits, controls, and logging. Furthermore, the report notes that electronic interfaces were not fully supported by memorandums of agreement. The vulnerabilities and risks of operating the Consolidated Analysis and Reporting System were not known because the system was not accredited to operate. During the course of the audit, system management validated the access requirements of users, began a draft of an instruction to require semiannual confirmation of access requirements, took action to obtain current memorandums of agreement, and stated that the risks involved with the utility program would be included as part of the final system accreditation decision, to be completed by February 28, 1998. Because of management actions, the report contained no recommendations.

Project No. 96054027, "Data Communications Security," April 15, 1997. The audit objective was to determine whether the Air Force adequately protected sensitive-but-unclassified information transmitted over the Air Force Internet. The report concludes that Air Force systems continued to transmit sensitive-but-unclassified information unprotected over the Air Force Internet because the Air Force system managers had not conducted a risk analysis. Users and system managers of 5 of the 11 systems examined were not aware of the increased risk of using the Air Force Internet or of the sensitive nature of the information. Air Force officials did not make staff aware of the open nature of the Air Force Internet, and system managers and users assumed that the Air Force Internet was protected.

The report recommended that management conduct a risk analysis for each system to identify the current risks of transmitting sensitive-but-unclassified information over the Air Force Internet, as well as emphasizing protection requirements to the designated approving authorities. Management concurred with the recommendations and planned to request that major commands, field operating agencies, and direct reporting units provide assurance that current certification and accreditation packages (including risk analysis) exist for all automated systems under their purview. Management also planned to review the certification and accreditation process that commands and designated approving authorities used for the 10 systems mentioned in the report. Management stated that it would distribute a message, citing specific policies and public law, to emphasize that the Air Force Internet is a nonsecure open system, subnets are responsible for securing their own sensitive-but-unclassified data, and certification and accreditation must be performed before fielding new systems. The report states that management actions should correct the problems.

Project No. 96066009, "Application Controls Within the Wholesale and Retail Receiving and Shipping System," March 14, 1997. The report states that system personnel did not adequately control system access. Specifically, 9 of 90 sampled users at 3 air logistics centers had user identifications and passwords allowing access to the Wholesale and Retail Receiving and Shipping System, although they no longer had a valid need for access.

The report recommended that the Air Force Materiel Command require system personnel to maintain a record of authorized users and periodically validate system access with users' supervisors and DISA access listings. Management concurred and agreed to issue guidance to implement the recommendations but stated that validating the large number of scattered users who were limited to read-only access was not necessary or practical. The report states that management's corrective actions were responsive.

As of March 31, 1997, management had issued a letter to all system sites reaffirming the need to annually validate all customers that had been granted access to the system to ensure that individuals with access were acting in the full capacity of their official duties.

Project No. 96066012, "Application Controls Within the Financial Inventory Accounting and Billing System," March 7, 1997. The report states that transaction controls were inadequate to prevent unauthorized changes to data, and controls were not adequate to prevent unauthorized access to the system. As a result, authorized users and programmers made unauthorized and untraceable changes to more than 1.4 million records from January 1995 through February 1996, and the Air Force had no assurance that only authorized personnel had access to the system. The office of primary responsibility for the system did not comply with access oversight controls.

The report recommended that the Director, DFAS, coordinate with the Air Force Materiel Command Director of Logistics to remove a query capability that allowed users to bypass transaction controls. Management agreed to control access to the query capability and to provide an audit trail. The report also recommended that the Director, DFAS, direct the offices of

primary responsibility at the air logistics centers to record and validate authorized user access. Management concurred and stated that it would reference the DFAS memorandum, "Implementation of System Access Oversight Controls for the Financial Inventory Accounting and Billing System," September 27, 1996, in the system user manual. The report states that management's planned actions were responsive.

Project No. 96066010, "Application Controls Within the Airlift Service Industrial Fund Integrated Computer System," August 23, 1996. The report states that the Airlift Service Industrial Fund Integrated Computer System is an integrated accounting and budgeting system that provides financial management support to the Air Mobility Command. The audit objective was to determine the adequacy of internal controls within the Airlift Service Industrial Fund Integrated Computer System. The report concludes that controls within the Airlift Service Industrial Fund Integrated Computer System needed improvement. The report states that data and system code were vulnerable to unauthorized modification or destruction. The office of primary responsibility for the system was unaware of the internal control weaknesses because of an inadequate system review.

The Air Mobility Command Comptroller concurred with the recommendations and agreed to remove a query update capability, incorporate controls to separate production data and application programs, and modify the Airlift Service Industrial Fund Integrated Computer System operating procedures.

The system contractor removed the query update capability from the Airlift Service Industrial Fund Integrated Computer System production region as of November 30, 1996. As of September 30, 1996, the contractor completed actions to restrict system access to both production data and application programs. In October 1996, the contractor completed actions to put the code used to update reports in the general ledger under formal configuration control. As of February 28, 1997, software had been modified for the capability of creating audit trails. Management submitted a request to the contractor for creating a transaction history file, and the estimated completion date was December 3, 1998.

Project No. 96054010, "General and Application Controls Within the Integrated Accounts Payable System," August 1, 1996. The report states that personnel at the Defense accounting offices and the operation location reviewed did not adequately control access to the Integrated Accounts Payable System, 10 locations did not review security transaction reports to detect unauthorized access, and 8 locations allowed personnel more access than necessary to perform their assigned duties. The report notes that management had not established guidance addressing Integrated Accounts Payable System access levels. The report also states that some users had access to both the Integrated Accounts Payable System and the Integrated Paying and Collecting System, resulting in the potential that a user could create fictitious accounts payable and fraudulently disburse Government funds to settle the accounts. Applicable directives did not specifically require supervisors to deny individuals simultaneous access to both systems, and management had not established guidance addressing access levels.

DFAS implemented desk procedures to deny individuals access to both systems, to control supervisor-level access, to direct supervisors and disbursing officers to comply with the Air Force directive requirement for daily review of security transaction reports, and to require DFAS Denver to implement the recommended procedures for field operation internal reviews as of March 6, 1997.

Project No. 95066023, "Followup Audit--Application Controls Within the Contract Depot Maintenance Production and Cost System," May 24, 1996. The report identifies application control weaknesses of the AFMC Contract Depot Maintenance Production and Cost System. The system did not have an adequate audit trail, air logistics center personnel did not properly limit user access to specific functions in all cases, and air logistics center personnel did not properly review access listings to determine whether users had a valid need to access the system. The office of primary responsibility for the system was unaware of the internal control weaknesses because of an inadequate system review.

The report recommended that DFAS design and implement a transaction history file, including altering system documentation to require retention of the file for at least 2 years. The report also recommended that DFAS direct the system's office of primary responsibility to implement procedures to maintain and reconcile lists of authorized users, limit user access to only those who have a need for specific data, and restrict programmer access so that the programmers cannot update production data. DFAS concurred with the recommendations and agreed to design a read-only transaction history file, require transaction histories to be kept for at least 2 years, require system personnel to maintain and reconcile a list of authorized users, reemphasize the criticalness of access control, and restrict the production data update capability through user identification.

The estimated completion date of the transaction history file slipped to October 1, 1998, dependent on completion of system reengineering. DFAS revised its instructions to require system personnel to maintain and reconcile a list of authorized users as of March 26, 1998. DFAS issued a memorandum to reemphasize the importance of access control and to restrict the production data update capability through user identification as of March 6, 1997.

Project No. 95066008, "Application Controls Within the Central Procurement Accounting System," May 10, 1996. The report states that the Central Procurement Accounting System (the Accounting System) records all stages of fund execution at Air Force Materiel Command (AFMC) base-level accounting offices. The audit objective was to determine the adequacy of internal controls within the Accounting System. The report concludes that Accounting System access controls and audit trails were not adequate to protect data integrity. The office of primary responsibility for the system was unaware of the internal control weaknesses because of an inadequate system review.

During the audit, the Air Force Audit Agency stated that the Accounting System should properly implement a software program already in use to prevent unauthorized personnel from accessing application programs. Management took steps to ensure that unauthorized users could not access the application

programs. Therefore, the report did not include a recommendation on that issue. The report recommended that AFMC remove the query data modification capability from the Accounting System production region. Management concurred and restricted the capability to update production data to authorized users only. The report also recommended that the Accounting System office of primary responsibility coordinate with AFMC to restrict program office personnel from accessing both accounting system application programs and the production database. Management concurred and agreed to restrict application and surveillance programmers from having the capability to change Accounting System production data.

Project No. 95066019, "Review of Application Controls Within the Depot Maintenance Production Cost System," October 24, 1995. The report states that the Depot Maintenance Production Cost System (G072A) provides the five AFMC air logistics centers visibility over depot maintenance revenue and related costs. The audit objective was to determine the adequacy of application controls within the G072A system. The report concludes that program and operational personnel did not maintain adequate separation of duties, did not control system access, and did not prepare and maintain sufficient documentation. System operators and application programmers could change or delete the job order number, labor, material, and overhead costs without creating a transaction history and audit trail. The report states that the G072A system office of primary responsibility was not aware that the access was a potentially serious breach of internal controls. The report notes that because of insufficient visibility over manual input transactions, more than 2,000 AFMC and DoD personnel had unrestricted access to create, modify, or delete input transactions to 47 AFMC and DoD systems, including the G072A system. The report explains that the G072A offices of primary responsibility at the air logistics centers did not maintain adequate control or accountability over users with access to the G072A system. As a result, the air logistics center offices of primary responsibility did not know whether only authorized individuals had access to G072A system data. The office of primary responsibility for the G072A system was unaware of significant internal control weaknesses because of an inadequate system review.

Management planned to coordinate with the Defense Information Systems Agency and AFMC to rescind update access to production data for system operators and application programmers. Management also planned to establish procedures and criteria to require the air logistics center offices of primary responsibility to approve, monitor, control, and periodically validate user access. Management's planned actions were on hold while AFMC evaluated the Navy Industrial Fund Management System to possibly replace the existing depot maintenance financial data processing systems. The Air Force granted approval on January 15, 1998, to replace AFMC legacy financial systems for depot maintenance, including the G072A system.

Project No. 95066021, "Review of H036A Controls Within the Depot Maintenance Business Area Cost Accounting and Production Report," September 15, 1995. The report concludes that users could alter cost or production data in any field to enhance the appearance of their work or to diminish the appearance of others' work. The incorrect and unsupported cost accounting data could affect major decisions on assigning work and retaining

depots, weapon systems, or both. The report did not include recommendations for further corrective actions because management initiated corrective actions during the audit. AFMC drafted sections of the users' manual to establish responsibility for reviewing, executing, and approving changes to fields in the "correct error" screen and for maintaining records of those actions.

Project No. 95066003, "Review of General Controls Over the Air Force Equipment Management System's Operating Systems," August 21, 1995. The report states that Air Force equipment managers used the Air Force Equipment Management System to determine new equipment needs and to account for and report existing equipment. The audit objective was to determine whether general controls over the operating systems and security software for the Air Force Equipment Management System were adequate to ensure operational continuity and support for Air Force missions. The report concludes that the Air Force Equipment Management System operating systems had software control weaknesses. Systems software personnel did not control user access to sensitive programs, data, and administrative authorities. Unauthorized users could compromise the integrity of Air Force Equipment Management System data by accessing the system, circumventing security controls, and manipulating the programs and data without detection. The report says that the Air Force Equipment Management System Program Management Office could not ensure that only authorized personnel had access to the classified and unclassified systems. Security administration personnel did not identify and delete all inactive identifications and had not established effective procedures to ensure a yearly revalidation of user identifications. As a result, program personnel could grant access to unauthorized users. The Air Force Equipment Management System did not include the capability to provide a complete audit trail of system activity. As a result, system operators could not trace potentially inappropriate activity to its source to initiate corrective action.

Because management corrected the identified operating systems and security software control weaknesses during the audit, no recommendations were in the report. The Air Force Equipment Management System Program Management Office issued guidance requiring system security administrators to review user privileges and restrict access on a need-to-know basis. System security administrators reviewed system administrative privileges and removed privileges from several users. The Program Management Office issued guidance requiring deletion of inactive user identification and improvement of annual user certification procedures. Also, management initiated actions that would result in the capability to produce complete audit trails.

Project No. 95066007, "Review of Application Controls Within the Maintenance Labor Distribution and Cost System," August 18, 1995. The report states that the Maintenance Labor Distribution and Cost System (G037G) provides the AFMC air logistics centers visibility over depot maintenance labor use and costs. The report concludes that AFMC had not implemented adequate controls over the G037G system, such as restricting programmer access to production data. System programmers could make unauthorized changes to labor-cost data, which would cause the G037G system to provide incorrect labor use and cost information for management reports and Defense Business Operations Fund financial statements. Because the operational locations did not retain transaction histories for the required 2-year period, management could

not trace transactions to ensure that they were properly authorized and accurate, properly and promptly accumulated in ledger accounts, and uniquely referenced to individual source records. The report states that the office of primary responsibility for the system was unaware of the internal control weaknesses because of an inadequate system review.

AFMC agreed to reconfigure the security software and also planned to establish controls to allow programmers access to production data when necessary, under the supervision of the system office of primary responsibility. Because the office of primary responsibility prepared a document addressing proper retention of transaction histories, the report contained no recommendations for additional action. AFMC sent a memorandum to the Air Force Audit Agency on January 5, 1996, which outlined separation-of-duty safeguards and controls, based on the controls over an existing system, that AFMC would implement on G037G.

Project No. 94066013, "Review of Application Controls Within the Project Order Control System," June 26, 1995. The report states that operational locations did not retain transaction histories for the required 2 years, and the Project Order Control System did not maintain adequate audit trails. The report notes that the office of primary responsibility for the system was unaware of the internal control weaknesses because of an inadequate system review. The report recommended that AFMC revise guidance and coordinate with the Defense Information Systems Agency to retain transaction histories for 2 years. The report also recommended that AFMC direct the system office of primary responsibility to establish clear audit trails within the system. AFMC concurred with the recommendations and stated that it would direct the system office of primary responsibility to implement actions to retain transaction histories for 2 years and to establish audit trails in the system. The audit report states that planned management actions were responsive.

As of July 31, 1996, the system office of primary responsibility had issued guidance with the requirement to extend file retention (audit trails and transaction histories) as described in the recommendations and management comments.

Project No. 94066006, "Risk Management of Depot Maintenance Computer Systems," April 17, 1995. The report states that depot managers at the five air logistics centers did not adequately manage risk for computers used to diagnose, maintain, and modify weapon systems. Of 143 computers reviewed, 104 were not accredited, and the accreditation documentation on the remaining 39 was incomplete or outdated. In addition, the report states that depot maintenance computer users and security officers had not received adequate security awareness training. The report concludes that, because of those conditions, managers did not have reasonable assurance that appropriate security measures were in place to protect data and computer systems, and depot maintenance managers did not understand how to accomplish risk assessments, resulting in incomplete risk assessments for 135 of 143 systems reviewed. The report lists specific deficiencies found, such as inadequate access controls, lack of guidance on protection of critical functions, lack of documentation of manufacturer certification of computer equipment, lack of separation of technical assessment

and accreditation duties, and the ability of system users to create classified information by aggregating unclassified data from different computer systems.

Management stated that Air Force Instruction 33-202, "Computer Security Program," would designate the commander of the major command as the designated approving authority for the command's automated systems. Existing AFMC guidance on certification and accreditation of computer systems requires commanders to establish a plan with milestones to achieve appropriate levels of accreditation, which included a determination of the possibility of data aggregation, for all nonaccredited or improperly accredited computer systems. AFMC issued guidance to define the responsibilities of system security personnel and to rate the personnel on their effectiveness. Regarding safeguards for critical processing, management stated that applicable guidance would be available in an upcoming certification and accreditation manual. Management also agreed to clarify the requirement of hardware and software certification documentation. AFMC was working on a system to provide computer security nonintelligence warning notices to depots. Finally, management agreed to issue guidance listing training areas and assigning responsibilities for establishing specific functional training and managing the training program.

Project No. 93058001, "Review of Personnel Concept III System Security and Equipment Management," April 3, 1995. The report concludes that the Air Force had limited assurance that the Personnel Concept III system was protected from unauthorized individuals entering, altering, reading, or copying sensitive personnel data. The Air Force Military Personnel Center did not establish adequate separation of duties, obtain required system and database accreditation, conduct system risk assessments, or establish effective access controls. The report states that personnel were either not aware of the database accreditation requirement or not complying with the requirement. The report notes that computer equipment accountability was inadequate, and equipment configuration was not properly managed and reported, making the equipment vulnerable to theft and misuse.

Air Force management officials agreed with the overall audit results and planned to incorporate separation-of-duty and consolidated accreditation database requirements into system policy and procedures. Revised guidance would provide details to the Computer System Security Officers on completing physical security risk analyses, as well as guidance on identifying system threats and vulnerabilities, establishing site-specific protective measures, and making suggestions on areas that may require additional protection. Management planned to issue guidance on password controls and to require system administrators to change root and firmware passwords regularly.

The Air Force Military Personnel Center incorporated separation of duties in the Computer System Security Support Plan, as updated on August 30, 1995. The Air Force Military Personnel Center modified the Computer System Security Support Plan to provide more comprehensive guidance to include accreditation guidelines and sample security operating instructions. Access controls, password controls, and equipment physical security and configuration management would be addressed in a change to Air Force Manual 36-2622.

Project No. 94066003, "Review of Computer Security at Air Force Materiel Command Laboratories," January 3, 1995. The report states that security controls over the AFMC laboratory network were inadequate to protect against unauthorized access. Laboratory computer security personnel did not perform adequate risk management, and laboratory computer security managers did not implement adequate general computer access controls. Deficiencies in general computer access controls included a lack of control over user privileges, inadequate contingency planning, and insufficient physical security.

Management agreed to prepare instructions for identifying vulnerabilities, reporting incidents, and performing system accreditation studies. Management cited existing criteria and systems that it would use for reporting security incidents; accounting for Government-owned computers; and tracking and performing the certification, accreditation, and risk assessment processes.

AFMC provided guidance and training on identifying known vulnerabilities, incident reporting procedures, audit trail review procedures, and security tools and configuration. AFMC also provided supplemental guidance and training on risk analysis and accreditation requirements.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Director, Information Assurance
Assistant Secretary of Defense (Public Affairs)
Director, Defense Logistics Studies Information Exchange

Joint Staff

Director, Joint Staff
  Director, Operations
  Director (Command, Control, Communications, and Computers)

Department of the Army

Chief Information Officer
Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Chief Information Officer
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
Office of Information and Regulatory Affairs
Technical Information Center, National Security and International Affairs Division, General Accounting Office

Chairman and ranking minority member of each of the following congressional committees and subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report.

Thomas F. Gimble
Patricia A. Brannin
Mary L. Ugone
Cecelia A. Miggins
Andrew J. Filer
Michael T. Carlson